DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

EMERGENCY ORDINANCE 155/2024
on the establishment of a framework for the cybersecurity of networks and information systems in the national civilian cyberspace
Monday 30 December 2024

Taking into account the fact that the rapid evolution and adoption of emerging technologies creates new types of interdependencies and exposes the critical infrastructure of the state to complex, previously unforeseen risks that are likely to generate significant effects on cybersecurity, effects that also extend to public administration authorities and institutions,

considering that the diversification and use of online services has seen a major acceleration due to several factors - including the Russian-Ukrainian conflict, the COVID-19 pandemic, the development and globalisation of the business environment, and the decreasing costs of accessing new markets – this shift has generated both benefits and a new spectrum of cybersecurity threats, risks and vulnerabilities, vulnerabilities that are intrinsically associated with smart technologies, such as 5G networks, the Internet of Things (IoT) and artificial intelligence (AI),

taking into account the fact that since the outbreak of the armed conflict in the vicinity of Romania, an increased use of cyber-attacks as part of military operations has been observed, with cross-border effects that also affect states not directly involved in the conflict - for example, the cyber-attack on the KA-SAT satellite communications network, operated by VIASAT, whose effects have expanded at European level, with their impact being felt in Romania as well,

also mentioning the involvement of new cyber actors in the conflict, including hacker groups supporting one of the sides involved in the conflicts, such as the Killnet Group, who carried out cyberattacks against essential infrastructures and services in European Union Member States supporting Ukraine, including Romania,

also taking into account the increase in the level of digitalisation and interconnection of information systems, corroborated with the development of the capabilities of malicious actors in the online environment, which has led to an intensification of incidents that generate a significant impact on infrastructures in areas of critical importance by compromising the supply chain,

highlighting major incidents, such as the one in the first quarter of 2024, which affected 26 hospitals nationwide, through a managed service provider, with a direct impact on the vital services offered to the population, which revealed the limits of the coverage of current legislation in the field of cybersecurity and the need to implement updated European regulations regarding supply chain security and the imposition of obligations for the management of entities, in order to increase their level of resilience, in correlation with their level of societal risk,

considering that the prompt adoption of the measures and mechanisms provided by the NIS2 Directive becomes imperative for increasing Romania's resilience to cyber threats, given the crucial role of this Directive in strengthening national cyber incident defence and response capacities, and also the application of the provisions of the NIS2 Directive contributes to Romania's alignment with international standards, thereby strengthening national capacity to react effectively to regional and global developments in cybersecurity,

taking into account the fact that the aspects presented constitute an objective, quantifiable and extraordinary state of affairs, independent of the will of the Government, that endangers the public interest and whose regulation cannot be postponed,

Pursuant to article 115 paragraph (4) of the Romanian Constitution, republished,

The Government of Romania adopts this emergency ordinance.

Chapter I General provisions

Section 1 Object and purpose

Article 1

This emergency ordinance establishes the legal and institutional framework, measures and mechanisms necessary to ensure a high common level of cybersecurity at national level.

Article 2

(1) The purpose of this emergency ordinance is:

a) the establishment of cybersecurity risk-management measures for national civilian cyberspace and incident reporting obligations for essential and important entities;

b) the establishment of the framework for cooperation at national level and participation at European and international level in the field of ensuring cybersecurity;

c) the designation of the National Cyber Security Directorate, hereinafter referred to as DNSC, as the competent authority responsible for cybersecurity and for the tasks of supervision and enforcement of measures for a high common level of cybersecurity, as well as other public or private law entities with competences and responsibilities in the application of the provisions of this emergency ordinance;

d) the designation of the single point of contact at national level and the national cybersecurity incident response team.

(2) This emergency ordinance does not apply to institutions in the field of defence, public order and national security, according to the provisions of art. 6 of Law no. 51/1991 on the national security of Romania, republished, with subsequent amendments and completions, to the Ministry of Foreign Affairs, to the Office of the National Register of State Secret Information and to the entities with attributions in the field of law enforcement, including the prevention, investigation, detection and prosecution of criminal offences. Information and communication systems that circulate classified information are also exempted from the application of this emergency ordinance.

(3) Entities to which Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of 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, hereinafter referred to as the DORA Regulation, applies, are only subject to the provisions of arts. 5-10 and 18.

(4) By exception to para. (2), in the event that entities within them act as a provider of trust services, the institutions in the field of defence, public order and national security, the Ministry of Foreign Affairs, as well as the Office of the National Registry of State Secret Information ensures the achievement of a common high level of cybersecurity by applying Law no. 58/2023 on Romania's cybersecurity and defence, as well as for amending and supplementing certain normative acts.

(5) This emergency ordinance applies without prejudice to the provisions of Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, with subsequent amendments and completions, Regulation (EU) 2016/679 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), Law no. 286/2009 on the Criminal Code, as subsequently amended and supplemented, and the legal provisions regarding the resilience of critical entities.

Section 2 Principles and definitions

Article 3

(1) In applying this emergency ordinance, the following principles are respected:

a) the principle of responsibility and awareness - consists of the continuous effort carried out by public and private law entities in raising awareness of the individual role and responsibility for achieving a high common level of cybersecurity at national level;

b) the principle of proportionality - consists of ensuring a balance between the risks to which networks and information systems are subjected and the security measures implemented;

c) the principle of cooperation and coordination - consists of carrying out the exchange of information regarding security risks to networks and information systems in a timely manner and ensuring the reaction to the occurrence of incidents in a synchronised manner;

d) the principle of minimising of effects - in the event of an incident, measures are taken to avoid amplifying or extending the effects to other networks and information systems;

e) The principle of satisfying the public interest – the satisfaction of the public interest is pursued before the individual or group interest.

(2) In application of this emergency ordinance, confidential information and trade secret information may be subject of information exchange with the European Commission and other authorities. The exchange of information is limited to relevant information, proportionate to the purpose pursued. The exchange of information preserves the confidentiality of that information and protects the security and commercial interests of the entities concerned.

Article 4

For the purposes of this emergency ordinance, the terms and expressions below have the following meanings:

a) cyber threat means a threat, as defined in art. 2 letter f) of the Government Emergency Ordinance no. 104/2021 on establishing the National Cyber Security Directorate, approved with amendments and completions by Law no. 11/2022, with subsequent amendments;

b) significant cyber threat means a cyber threat that can be assumed, based on its technical characteristics, to have the potential to seriously affect an entity's network and information systems or the users of the services provided by the entity, causing considerable material or moral damage;

c) cybersecurity audit, as defined in art. 2 letter d) of Law no. 58/2023;

d) sectoral competent authority in the field of cybersecurity is that public institution that has either a regulatory role or a supervisory and control role, or a regulatory, supervisory and control role in the areas corresponding to the sectors provided for in the annexes and which, according to the competences and attributions established by the normative acts of its own organisation and functioning, has attributions in the field of cybersecurity at the level of the entities within the sectors provided in Annexes 1 and 2;

e) cyber crisis, as defined in art. 2 letter k) of the Government Emergency Ordinance no. 104/2021;

f) entity means a natural or legal person constituted and recognised as such under the domestic law of its place of establishment, which may, acting in its own name, exercise rights and be subject to obligations;

g) public administration entity means an authority or institution of the public administration, according to the provisions of art. 5 letters k), l), w) and kk) of the Government Emergency Ordinance no. 57/2019 on the Administrative Code, as subsequently amended and supplemented, as well as an administrative-territorial unit, a public law body or an association formed by one or more such public sectors authorities or institutions or by one or more such public law bodies;

h) entity providing domain name registration services means a registry operator or an agent acting on behalf of registry operators, such as a provider or reseller of privacy protection services or proxy services;

i) DNS service provider means an entity that provides:

1. publicly available recursive domain name resolution services for internet end-users;
2. authoritative domain name resolution services intended for use by third parties, except root name servers;

j) managed service provider means an entity that provides services related to the installation, management, operation or maintenance of information and communication technology products, networks, infrastructures or applications, hereinafter referred to as ICT, or other networks and information systems, through active assistance or administration, either at the customer's premises or remotely;

k) managed security service provider means a managed service provider that performs or provides assistance for activities related to cybersecurity risk-management;

l) incident management means all actions and procedures aimed at preventing, detecting, analysing and limiting an incident or aimed at responding to it and recovering from the incident;

m) incident means an event that compromises the availability, authenticity, integrity or confidentiality of the data stored, transmitted or processed or of the services offered by or accessible through computer networks and systems;

n) large-scale cybersecurity incident means an incident that causes disruption beyond the response capabilities of a single Member State of the European Union or that has a significant impact on at least two Member States of the European Union;

o) near miss incident means an event that could have compromised the availability, authenticity, integrity or confidentiality of the data stored, transmitted or processed or of the services offered by or accessible through networks and information systems, but which was successfully prevented from materializing or which did not materialize;

p) internet exchange point means a network facility that allows the interconnection of more than two independent autonomous networks, in particular for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which does not require internet traffic between any pair of participating autonomous systems to pass through a third autonomous system, nor does it modify or otherwise interact with that traffic;

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

r) research organisation means an entity whose main objective is to carry out applied research or experimental development activities in order to exploit the results of that research for commercial purposes, but which does not include educational institutions;

s) conformity assessment body means the body referred to in art. 2 para. (13) of Regulation (EC) no. 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) no. 339/93;

t) national accreditation body means the body referred to in art. 2 para. (11) of Regulation (EC) no. 765/2008;

u) online marketplace means a service, as defined in art. 2 letter o) of Law no. 363/2007 on combating unfair practices of traders in relation to consumers and harmonizing regulations with European legislation on consumer protection, with subsequent amendments and completions;

v) social networking service platform means a platform that allows end-users to connect, share, discover and communicate with each other across multiple devices, including through online conversations, posts, videos and recommendations;

w) information systems and network security policy means a policy that establishes the security measures for information networks and systems that must be adopted by an essential or important entity;

x) trust service provider means a trust service provider within the meaning of art. 3 para. (19) of Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;

y) qualified trust service provider means a qualified trust service provider within the meaning of art. 3 para. (20) of Regulation (EU) no. 910/2014;

z) ICT process means an ICT process within the meaning of art. 2 para. (14) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) no. 526/2013 (Cybersecurity Act);

aa) ICT product means an ICT product within the meaning of art. 2 para. (12) of Regulation (EU) 2019/881;

bb) TLD name registry means an entity to which a specific top-level domain has been delegated and which is responsible for the administration of the top-level domain, including the registration of domain names under the top-level domain and the technical operation of the top-level domain, including the operation of its name servers, the maintenance of its databases and the distribution of top-level domain area files between name servers, regardless of whether it is carried out by the entity itself or outsourced, but excluding situations where top-level domain names are used by a registry exclusively for its own use;

cc) representative means a natural or legal person established in the European Union who is expressly designated to act on behalf of a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, an online marketplace provider, an online search engine provider or a social networking service platforms provider that is not established in the European Union, who may be contacted by the competent cybersecurity authority in the field of cybersecurity in relation to that entity's obligations under the provisions of this emergency ordinance;

dd) content delivery network means a geographically distributed network of servers designed to ensure the high availability, accessibility or rapid provision of digital content and services to internet users on behalf of content and service providers;

ee) public electronic communications network means a public electronic communications network within the meaning of art. 4 para. (1) point 10 of the Government Emergency Ordinance no. 111/2011 on electronic communications, approved with amendments and completions by Law no. 140/2012, with subsequent amendments and completions;

ff) network and information system means:

1. electronic communications network within the meaning of the provisions of art. 4 para. (1) point 6 of the Government Emergency Ordinance no. 111/2011;
2. any device or set of interconnected or functionally related devices, one or more of which ensures the automatic processing of digital data with the help of a computer program; or
3. digital data stored, processed, retrieved or transmitted by the elements provided for in points 1 and 2 for their operation, use, protection and maintenance;

gg) risk means the potential for loss or disruption caused by an incident and must be expressed as a combination of the magnitude of such loss or disruption and the probability of the incident occurring;

hh) cybersecurity means cybersecurity, as defined in art. 2 letter y) of Law no. 58/2023 on Romania's cybersecurity and defence, as well as for amending and completing some normative acts;

ii) security of networks and information systems means the capacity of networks and information systems to withstand, at a certain level of trust, any event that could compromise the availability, authenticity, integrity or confidentiality of the data stored, transmitted or processed or of the services provided by these networks and information systems made available;

jj) digital service means a service within the meaning of the provisions of art. 4 para. (1) point 2 of the Government Decision no. 1016/2004 regarding the measures for the organisation and implementation of the exchange of information in the field of technical standards and regulations, as well as the rules regarding information society services between Romania and the Member States of the European Union, as well as the European Commission, with subsequent amendments and completions;

kk) data centre service means a service that comprises structures or groups of structures dedicated to the hosting, interconnection and centralized exploitation of IT and network equipment that provides data storage, data processing and transport, together with all the facilities and infrastructures for power distribution and environmental control;

ll) cloud computing service means a digital service that enables on-demand administration and broad remote access to a scalable and variable set of IT resources that can be shared, including in the event that the respective resources are distributed in different locations;

mm) electronic communications service means an electronic communications service within the meaning of art. 4 para. (1) point 9 of the Government Emergency Ordinance no. 111/2011;

nn) trust service means a trust service within the meaning of art. 3 para. (16) of Regulation (EU) no. 910/2014;

oo) qualified trust service means a qualified trust service within the meaning of art. 3 para. (17) of Regulation (EU) no. 910/2014;

pp) ICT service means an ICT service within the meaning of art. 2 para. (13) of Regulation (EU) 2019/881;

qq) domain name system or DNS means a hierarchical distributed naming system that enables the identification of internet services and resources, that allows end-user devices to use internet routing and connectivity services to reach these services and resources;

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

ss) standard means a standard within the meaning of art. 2 para. (1) of Regulation (EU) no. 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision no. 1673/2006/EC of the European Parliament and of the Council;

tt) vulnerability means a weakness, susceptibility or deficiency of ICT products or ICT services that can be exploited by a cyber threat.

Chapter II Scope

Section 1 Essential entities

Article 5

(1) The following entities are considered essential, regardless of their size:

a) central public administration entities in accordance with Annex 1;

b) entities in Annex 1 or 2 identified in accordance with art. 9;

c) entities identified as critical entities according to the legal provisions regarding the resilience of critical entities;

d) DNS service providers;

e) qualified trust service providers;

f) TLD name registries.

(2) Entities in the category of large enterprises according to art. 8 and falling within the sectors provided for in Annex 1 are considered essential.

(3) Entities in the category of medium-sized enterprises according to art. 8 and which are providers of public electronic communications networks or providers of electronic communications services intended for the public are considered essential.

(4) Entities in the category of medium-sized enterprises according to art. 8 and which are providers of managed security services are considered essential.

Section 2 Important entities

Article 6

(1) Entities in the categories of large and medium-sized enterprises according to art. 8, which fall under Annexes 1 and 2 and which are not identified as essential entities pursuant to art. 5, are considered important entities.

(2) The following entities are considered important if they have not been identified as essential entities according to art. 5 and regardless of their size:

a) entities in Annexes 1 and 2 identified in accordance with art. 9;

b) providers of public electronic communications networks and providers of publicly available electronic communications services;

c) trust service providers.

Section 3 Special provisions

Article 7

(1) The entities falling within the scope of this emergency ordinance are the entities in the sectors provided for in Annexes no. 1 and 2, established and registered on the territory of Romania according to the legal provisions.

(2) By exception from para. (1), providers of public electronic communications networks or providers of electronic communications services intended for the public falls within the scope of this emergency ordinance when they provide services on the territory of Romania, regardless of the place of establishment or registration.

(3) DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines and network social media service platforms fall within the scope of the of this emergency ordinance when their main establishment in the European Union is located on the territory of Romania.

(4) Foreign public administration entities are under the jurisdiction of the state that established them.

(5) For the purposes of this emergency ordinance, the main establishment as referred to in para. (3) is determined as follows:

a) is the establishment where decisions related to cybersecurity risk-management measures are predominantly made;

b) when the main establishment cannot be established according to letter a) or if such decisions are not taken in the European Union, it is considered to be the establishment where it carries out its cybersecurity operations;

c) when the main establishment cannot be determined according to letter b), it is considered to be in the state where the entity in question has its registered establishment with the largest number of employees.

(6) When, in the situation described in para. (3), the entity is not established in the European Union, but provides/offers services on its territory, the entity is obliged to appoint a representative in the European Union, within one of the Member States in which it provides its services. In this case, the entity is considered to be under the jurisdiction of the Member State in which the representative is established.

(7) When the entity provides services on the territory of Romania, DNSC may bring legal action according to the legal provisions against the entity in question for non-compliance with the provisions of this emergency ordinance, including in the event that the entity has not appointed a representative pursuant to para. (6).

Article 8

(1) An entity is considered a large enterprise if it exceeds the criteria established for medium-sized enterprises as provided for in art. 4 para. (1) letter c) of Law no. 346/2004 on stimulating the establishment and development of small and medium-sized enterprises, with subsequent amendments and completions, without, however, applying the provisions of art. 4^5 of the same law.

(2) An entity is considered a medium-sized enterprise if it meets the criteria provided for in art. 4 para. (1) letter c) of the law referred to in para. (1), without however applying the provisions of art. 4^5 of the same law.

Article 9

An entity is considered essential or important if:

a) the entity is the only provider of a service that is essential for supporting critical societal and economic activities;

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

c) the disruption of the service provided by the entity generate a significant systemic risk, in particular for sectors where such a disruption could have a cross-border impact;

d) the entity is critical due to its specific importance at national or regional level for the sector or type of services concerned or for other interdependent sectors.

Article 10

(1) The determination of the impact generated by the disruption of the service provided by the entity, referred to in art. 9, is carried out depending on:

a) the impact on fundamental rights and freedoms;

b) the impact on the national economy;

c) the impact on people's health and life;
d) financial impact
e) the impact on defence, public order and national security;
f) cross-sectoral or cross-border impact.

(2) The criteria provided for in para. (1), their corresponding thresholds and the methodology for assessing the risk level of the entities are established by order of the Director of DNSC.

Chapter III Cybersecurity risk-management measures and reporting obligations

Article 11

(1) Essential entities and important entities take proportionate and appropriate technical, operational and organisational measures to identify, assess and manage the risks related to the security of the networks and information systems they use in carrying out their activities or providing their services, as well as to eliminate or, where appropriate, reduce the effects of incidents on the recipients of their services and other services.

(2) The measures provided for in para. (1) must ensure a level of cybersecurity appropriate to the level of risk of the entity, taking into account the current state of technology and, where appropriate, the most relevant national, European and international standards and best practices, as well as the costs of implementing these measures.

(3) The risk level of the entity is assessed according to the methodology for assessing the risk level of the entities included in the order of the Director of DNSC provided for in art. 10 para. (2).

(4) The measures provided for in para. (1) must include a comprehensive approach to cyber threats in order to ensure the protection of networks and information systems both logically and physically against incidents, including by logging and ensuring traceability of all activities within networks and information systems.

(5) Essential entities and important entities are obliged to undergo a cybersecurity audit under the conditions and with the periodicity established by the order of the Director of DNSC provided for in art. 12 para. (1), depending on the level of risk referred to in para. (3).

(6) When there is an authority with sectoral competences, the conditions and periodicity of the security audit provided for in para. (5) will be established by joint order under the conditions of art. 37 para. (8) letter b), depending on the level of risk referred to in para. (3).

(7) Essential and important entities provide to DNSC, upon request, the list of relevant assets and the list of risks identified following the risk analysis, provided for in para. (1).

(8) With regard to the security of the supply chain, the measures provided for in para. (1) must take into account:

a) the specific vulnerabilities of each direct provider and service provider, the overall quality of products and the quality of the cybersecurity practices of direct providers and service providers, including the security of their development processes;

b) the results of the coordinated risk assessments carried out taking into account the results of the coordinated risk assessments on critical supply chain security developed at European Union level within the Cooperation Group.

(9) In order to ensure the security of the supply chain, essential entities and important entities are under the obligation to transmit to DNSC, upon request, data on trust service providers, qualified trust service providers, DNS service providers, TLD name registries or entities offering domain name registration services, cloud computing service providers, data centre service providers, managed service providers and managed security service providers and providing them with these types of services, within the term provided in the DNSC request.

(10) When assessing the proportionality of the risk-management measures in accordance with the provisions of para. (1), appropriate account is taken of the extent of the entity’s risk exposure and the services it provides, the size of the entity, the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

Article 12

(1) The Director of DNSC issues an order regarding the risk-management measures provided for in art. 11 para. (1) with regard to the technical, operational and organisational requirements, according to art. 13.

(2) Without prejudice to the provisions of art. 37 para. (8) letter b) and para. (17), the order issued according to para. (1) may also include sector-specific requirements for these risk-management measures following consultation with the sectoral competent authorities with regulatory powers.

(3) If the management bodies of essential entities and important entities find that they do not comply with the measures provided for in the order referred to in para. (1) or, as the case may be, those provided for in the order referred to in art. 37 para. (8) letter b), they apply, without undue delay, the necessary corrective measures.

(4) Essential entities and important entities carry out and submit to DNSC and, as the case may be, to the sectoral competent authority, on an annual basis, a self-assessment of the maturity level of cybersecurity risk-management measures in accordance with the order provided for in para. (1) or, as the case may be, according to the order referred to in art. 37 para. (8) letter b), assumed by the management of the entity.

(5) Within 30 days of the self-assessment, the essential entities prepare and submit to DNSC and, where applicable, to the sectoral competent authority, a plan of measures to remedy the identified deficiencies, assumed by the entity's management, in accordance with the risk-management measures applicable to them.

Article 13

The measures provided for in art. 11 para. (1) include at least the following:

a) policies and procedures relating to risk analysis and security of information systems and their periodic review;

b) the policies and procedures for assessing the effectiveness of cybersecurity risk-management measures;

c) the policies and procedures relating to the use of cryptography and, where applicable, encryption;

d) supply chain security, including security aspects of the relationship between the entity and its direct providers and suppliers;

e) security of the acquisition, development, maintenance and decommissioning of networks and information systems, including vulnerability management and disclosure;

f) human resources security, access control policies and asset management;

g) incident management;

h) business continuity, including back-up management, disaster recovery and crisis management;

i) basic cyber hygiene practices and cybersecurity training;

j) the use of multi-factor authentication or continuous authentication solutions for voice, video and text communications, secure emergency communication systems within the entity, as appropriate.

Article 14

(1) The management bodies of essential entities and important entities approve the cybersecurity risk management measures they take in order to comply with arts. 11 to 13 and, where applicable, with the provisions of the joint order provided for in art. 37 para. (8) letter b), supervise their implementation and are responsible for violations of these provisions, without prejudice to the legal provisions on the liability of public institutions, public officials and those elected or appointed.

(2) Members of the management bodies of essential entities and important entities undergo accredited professional training in order to ensure a sufficient level of knowledge and skills to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity. The essential and important entities provide professional training to all staff in order to ensure a sufficient level of knowledge and skills.

(3) The management bodies of essential entities and important entities establish permanent means of contact, ensure the allocation of the necessary resources for the implementation of cybersecurity risk-management measures and, where appropriate, designate the persons responsible for the security of the networks and information systems in charge of implementing and supervising the cybersecurity risk-management measures at the level of the entity.

(4) The person responsible for the security of networks and information systems, provided for in para. (3), designated within the essential entities, except for public administration entities, as well as micro and small enterprises, as established according to the provisions of art. 4 para. (1) letters a) and b) of Law no. 346/2004, must cumulatively fulfil at least the following:

a) has managerial authority;

b) is directly subordinated to the management bodies of the entity;

c) operates independently from the IT and operational technology structures within the entity;

d) has access to the necessary resources for the effective supervision and implementation of cybersecurity risk-management measures;

e) to have obtained an accredited specialised course, recognised by DNSC, in the field of cybersecurity, within 12 months of designation.

Article 15

(1) Essential entities and important entities report, without undue delay, to the national cybersecurity incident response team, any incident that has a significant impact on the provision of their services and, where appropriate, the entities concerned notify, without undue delay, the recipients of their services of significant incidents that could affect the provision of those services.

(2) The reporting is done through the National Platform for Reporting Cyber Security Incidents, hereinafter referred to as PNRISC, as provided for in art. 20 of Law no. 58/2023.

(3) Critical entities and important entities report without undue delay, but no later than 6 hours after becoming aware of any information that enables the national cybersecurity incident response team to ascertain a cross-border impact of the incident. Mere reporting does not expose the entity to increased liability.

(4) In the event of a significant cross-border incident, the national single point of contact ensures that the counterpart authorities of those states receive the relevant information reported in a timely manner, according to para. (7).

(5) Where applicable, critical entities and significant entities, without undue delay, communicate to the recipients of their services that may be affected by a significant cyber threat, any actions or remedies that those recipients may take in response to that threat and, where applicable, the entities also inform the recipients concerned of the material threat itself.

(6) An incident is considered significant, or the impact of an incident is considered significant if:

a) it has caused or is likely to cause serious operational disruption to services or financial loss to the entity concerned;

b) it has affected or may affect other natural or legal persons, causing considerable material or non-material damage.

(7) For the purpose of reporting pursuant to para. (1), the entities concerned submit to the national cybersecurity incident response team:

a) without undue delay, but no later than 24 hours from the date on which they became aware of the significant incident, an early warning which, where appropriate, indicates whether there is suspicion that the incident is caused by unlawful or malicious actions or that it could have a cross-border impact;

b) without undue delay, but no later than 72 hours from the moment they became aware of the significant incident, a report of the incident, which, where appropriate, updates the information referred to in letter a) and provides an initial assessment of the significant incident, including its severity and impact, as well as indicators of compromise, if available;

c) an interim report on the relevant update of the situation, at the request of the national cybersecurity incident response team;

d) a final report, no later than one month after the submission of the notification of the incident pursuant to letter b), including at least the following elements:

1. a detailed description of the incident, including its severity and impact;
2. the type of threat or root cause that likely triggered the incident;
3. mitigation measures applied and ongoing;
4. where applicable, the cross-border impact of the incident.

e) in the case of an incident in progress at the time of submission of the report referred to in letter d), the entities concerned should submit a progress report, and a final report within one month of the incident being handled.

(8) By exception to para. 7 letter b), a trust service provider reports, in respect of material incidents affecting the provision of its trust services, to the national cybersecurity incident response team without undue delay and, in any event, within 24 hours of the date on which it became aware of the significant incident.

(9) The national cybersecurity incident response team provides, without undue delay and, where possible, within 24 hours of receiving the early warning according to para. (7) letter a), a response to the reporting entity, including an initial response to the significant incident and, at the request of the entity, guidance or operational instructions on the implementation of possible mitigation measures.

(10) The national cybersecurity incident response team may provide additional technical support if requested by the entity concerned. Where the incident is deemed to be of a criminal nature, the National Cyber Security Incident Response Team also provides guidance on the referral of the incident to criminal prosecution bodies.

(11) Where appropriate, and in particular where the significant incident involves two or more states, DNSC , without undue delay, informs the other affected states and the European Union Agency for Cybersecurity, hereinafter referred to as ENISA, of the significant incident. This information includes the type of information received according to para. (7).

(12) In the case of para. (11), DNSC, in accordance with national law and European Union norms, protects the security and commercial interests of the entity, such as privileged information, business-related data and ensures the confidentiality of the information provided.

(13) Where public awareness is necessary to prevent a significant incident or to manage an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, DNSC or, where applicable, DNSC together with its counterpart authorities in other concerned states may, after consulting that entity, inform the public of the material incident or require the entity to do so.

(14) The national single point of contact submits, where appropriate, the reports received according to para. (1) to the single points of contact from the other affected Member States.

(15) The national single point of contact transmits to ENISA, every three months, a summary report including aggregated anonymised data on significant incidents, incidents, cyber threats and near-miss incidents reported according to para. (1) and with those regarding voluntary reporting.

(16) DNSC provides to the National Coordination Centre for the Protection of Critical Infrastructures, hereinafter referred to as CNCPIC, information on significant incidents, incidents, cyber threats and near-miss incidents reported according to para. (1) and with the provisions regarding voluntary reporting by entities identified as critical entities under the legal provisions on the resilience of critical entities.

(17) Without prejudice to the provisions of art. 37 para. (8) letter b), by order of the Director of DNSC, methodological norms regarding the reporting of incidents are established.

Article 16

(1) Can report to the national cybersecurity incident response team:

a) critical entities and important entities, regarding incidents, cyber threats and near-miss incidents;

b) entities other than those referred to in letter a), regardless of whether they fall within the scope of this emergency ordinance, in respect of significant incidents, cyber threats and near-miss incidents.

(2) The voluntary reporting referred to in para. (1) is carried out in accordance with art. 15.

(3) The national cybersecurity incident response team prioritise the processing of mandatory notifications over voluntary notifications.

(4) Voluntary reporting does not impose any additional obligation on the notifying entity that would not have been imposed on it had it not submitted the reporting.

Article 17

By way of derogation from the provisions of art. 21 para. (1) and (2) of Law no. 58/2023, the persons provided for in art. 3 para. (1) letters b) and c) of the same law, that are identified as essential entities and important entities, apply the provisions of arts. 15 and 16 on incident reporting.

Chapter IV Record

Section 1 Register of entities

Article 18

(1) DNSC maintains a register of essential entities and identified important entities.

(2) Entities operating in the sectors listed in Annex 1 or Annex 2 notifies DNSC for registration no later than 30 days from the date of entry into force of this emergency ordinance or no later than 30 days from the date on which the provisions of this emergency ordinance are applicable to them, when, according to arts. 5 and 6, they qualify as essential entities or important entities.

(3) The notification referred to in para. (2) consists in providing DNSC with the following types of information:

a) name;

b) the address of the main establishment and up-to-date contact details, including email addresses and telephone numbers;

c) the addresses of the other registered offices in the European Union, as the case may be;

d) the permanent means of contact and the person within the entity in charge of monitoring the means of contact;

e) the person designated as the entity's representative, its address and contact details, if the entity is not established in the European Union;

f) sector, subsector and type of entity as set out in Annex 1 or Annex 2;

g) Member States in which they provide services, where applicable;

h) the entity's public IP address ranges, in the case of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, content delivery network operators, data centre service providers, managed service providers, managed security service providers, and digital service providers;

i) the public IP address ranges of the entity, for entities other than those provided for in letter h), as applicable;

j) necessary and sufficient information demonstrating the fulfilment of the conditions for identification as an essential entity or an important entity according to arts. 5 and 6 respectively.

(4) Within 60 days from the receipt of the notification provided for in para. (2), the DNSC Management issue a decision for the identification and registration of essential entities.

(5) Within 150 days from the receipt of the notification provided for in para. (2), the DNSC Management issue a decision for the identification and registration of important entities.

(6) Within 60 days from the date of communication of the decision of the Director of DNSC provided for in para. (4), respectively para. (5), essential entities and important entities submit the assessment of the entity's risk level to DNSC, in accordance with art. 10 para. (2).

(7) Within 60 days from the submission of the risk level assessment provided for in para. (6), the entities carry out a self-assessment of the maturity level of the cybersecurity risk-management measures provided for in art. 12 para. (4).

(8) The entities provided for in para. (2) communicate to DNSC the changes to the information provided for in para. (3), as follows:

a) For the information provided for in para. (3) letters a)-d), letters f) and j), without undue delay and, in any case, not later than 2 weeks from the day of the amendment;

b) For the information provided for in para. (3) letter e) and letters g)-i), without undue delay and, in any case, not later than 3 months after the date of the amendment.

(9) By order of the Director of DNSC, the requirements relating to para. (3) are laid down, including the method of transmission of information and the use of forms.

(10) The national single point of contact transmits, in relation to DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, content delivery network operators, data centre service providers, managed service providers, managed security service providers and digital service providers, the information referred to in para. (3) to ENISA, after receiving it, with the exception of the information contained in para. (3) letters i) and j) until 17 January 2025 at the

latest and whenever there are changes in relation thereto. The single point of contact reviews the required information regularly and at least every two years. By 17 April 2025 and upon request of the European Commission, the national single point of contact notifies the European Commission the names of essential and important entities identified according to art. 9.

(11) The entity ensures that it can be contacted using the contact details transmitted in accordance with para. (3).

(12) After the expiry of term provided for in para. (2), DNSC, ex officio or following a referral concerning a failure/subtraction to notify and enter in the register made by any concerned person, notify the entity in question of its obligation to undergo the identification process for registration in the register of essential or important entities.

(13) The entities that no longer meet the conditions and criteria set out in the provisions of this Emergency Order notifies DNSC for removal from the register and provides documentary evidence for this within 30 days of the date on which the changes are noted.

(14) DNSC orders, by decision of the management, the removal from the register following the assessment of the documentation provided for in para. (13) and communicates the decision to the entity.

(15) Entities may request the assistance of DNSC with regard to the process of identification, modification or deregistration.

(16) When an entity also provides an essential service within other Member States of the European Union, DNSC consults the corresponding authorities of those states before a decision on deregistration is taken.

(17) Entities other than those referred to in para. (2) may also be registered with DNSC, irrespective of their size, in accordance with para. (2) to (16).

(18) In order to carry out their duties, sectoral competent authorities may request and obtain, free of charge, following the conclusion of a protocol, information on data recorded in the register of essential and important entities corresponding to their fields of activity, in compliance with the legislation in force, in particular on the protection of personal data.

Article 19

(1) In order to contribute to the security, stability and resilience of domain name systems, TLD name registries and entities providing domain name registration services exercise due diligence to collect accurate and complete domain name registration data in a dedicated database, in accordance with European Union data protection law.

(2) A database according to para. (1) contains the information necessary to identify and contact the holders of domain names and contact points managing the domain names in the TLD and includes the following:

a) the domain name;

b) registration date;

c) the name, email address and telephone number of the registrant;

d) contact email address and telephone number of the contact point managing the domain name, if different from the registrant.

(3) TLD name registries and entities providing domain name registration services establish policies and procedures, including verification procedures, to ensure that the databases referred to in para. (1) contain accurate and complete information and make these policies and procedures publicly available.

(4) TLD name registries and entities providing domain name registration services make the non-personal domain name registration data publicly available immediately after the registration of a domain name.

(5) To the extent that the data provided by the domain name holder is incorrect, inaccurate or incomplete, TLD name registries and entities providing domain name registration services notify the right holder of the domain name in order to make available the correct, accurate and complete data within the time limit communicated.

(6) If the term granted according to para. (5) is not respected, the domain name is blocked.

(7) The transfer of a blocked domain name is prohibited and when the requested data has not been properly corrected, the domain name is cancelled.

(8) TLD name registries and entities providing domain name registration services provide access to the requested domain name registration data, upon duly substantiated and duly substantiated lawful requests, to persons who justify a legitimate interest according to the legal provisions.

(9) TLD name registries and entities providing domain name registration services make data disclosure policies and procedures publicly available and respond to all access requests expeditiously, but no later than 72 hours after receipt of a request.

(10) TLD name registries and entities providing domain name registration services cooperate with each other, including in order to avoid overlaps in the collection of domain name registration data, in the context of fulfilling the obligations provided for in para. (1) to (9).

(11) DNSC may request access to domain name registration data on a reasoned basis and conclude appropriate protocols with TLD registry operators and domain name registration service providers.

Section 2 Exchange of cybersecurity information

Article 20

(1) Essential, important and, where relevant, other entities may share relevant cybersecurity information with each other, on a voluntary basis, including information related to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat actor-specific information, cybersecurity alerts and recommendations on the configuration of cybersecurity tools to detect cyber-attacks.

(2) The information provided for in para. (1) is carried out within associations of essential and important entities and, where applicable, their providers or service providers, by means of cybersecurity information-sharing agreements, in compliance with all provisions on the protection of personal data.

(3) The exchange of information is carried out for the following purposes:

a) preventing and detecting, responding to or recovering from incidents or mitigating their impact;

b) enhancing the level of cybersecurity, in particular by raising awareness of cyber threats, limiting or preventing the possibility of the spread of such threats, supporting the range of defensive capabilities, remediating and disclosing vulnerabilities, detecting threats, threat containment and prevention techniques, mitigation strategies or stages of response and recovery processes, or promoting collaboration between public entities, and in the field of cyber threat research.

(4) Cybersecurity information exchange agreements also include information on operational elements, including the use of dedicated ICT platforms and automation tools, the content and conditions of the information exchange agreements, and DNSC is notified of both their conclusion and withdrawal.

(5) DNSC may support interested entities in concluding an agreement on the exchange of cybersecurity information and may request the limitation of the exchange of information when they refer to information made available by competent authorities or cybersecurity incident response teams.

Chapter V Roles and responsibilities

Section 1 Coordination at national level

Article 21

(1) The vision, the main guidelines and the general approaches regarding the field of cybersecurity at national level are defined and assumed in the Cyber Security Strategy of Romania, approved by Government Decision no. 1321/2021 on the approval of Romania's Cybersecurity Strategy, for the period 2022-2027, as well as the Action Plan for the implementation of Romania's Cyber Security Strategy, for the period 2022-2027, hereinafter referred to as the Strategy, and in the Action Plan for its implementation.

(2) The general framework for cooperation in the field of cybersecurity at national level is the National Cyber Security System, hereinafter referred to as SNSC, in accordance with the provisions of Law no. 58/2023.

Article 22

(1) The national cybersecurity strategy is developed by DNSC, in consultation with the other authorities with responsibilities in the field of cybersecurity according to the provisions of Law no. 58/2023, with the approval of the Cyber Security Operational Council, hereinafter referred to as COSC, and is adopted by Government decision, together with the action plan for the implementation of the strategy, which is annexed to it.

(2) In developing or updating the national cybersecurity strategy, DNSC may request ENISA's assistance.

(3) The national cybersecurity strategy sets out the strategic objectives, the resources necessary to achieve those objectives and the appropriate policy and regulatory measures to achieve and maintain a high level of cybersecurity.

(4) The national cybersecurity strategy is evaluated regularly and at least every five years on the basis of key performance indicators and, if necessary, updated and adopted following the same mechanism.

(5) Within three months from the date of adoption of the national cybersecurity strategy, DNSC submits it to the European Commission.

Article 23

(1) The national cybersecurity strategy developed according to art. 22 includes at least the following:

a) the objectives and priorities of the national cybersecurity strategy, covering in particular the sectors referred to in Annexes 1 and 2;

b) a governance framework for the achievement of the objectives and priorities referred to in letter a), including public policies;

c) a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, supporting cooperation and coordination at national level between competent authorities, single points of contact and cybersecurity incident response teams under this emergency ordinance, as well as coordination and cooperation between those bodies and competent authorities under sector-specific legal acts of the European Union;

d) a mechanism to identify relevant assets and a risk assessment at national level;

e) an identification of measures to ensure national incident preparedness, response capacity and recovery, including public-private cooperation;

f) a list of the different authorities and stakeholders participating in the implementation of the National Cyber Security Strategy;

g) a policy framework to ensure better coordination between competent authorities under this emergency ordinance and the legal provisions on the resilience of critical entities for the purpose of exchanging information on risks, cyber threats and incidents, as well as on risks, threats and non-cyber incidents and carrying out supervisory tasks, as appropriate;

h) a plan including the measures needed to raise citizens' overall awareness of cybersecurity.

(2) The national cybersecurity strategy provides for at least the following public policies:

a) addressing supply chain cybersecurity for ICT products and ICT services used by entities to provide their services;

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

c) vulnerability management, including promoting and facilitating coordinated disclosure of vulnerabilities;

d) related to maintaining the overall availability, integrity and confidentiality of the public core of the open internet, including the cybersecurity of submarine communications cables, where appropriate;

e) promoting the development and integration of relevant advanced technologies aimed at implementing state-of-the-art cybersecurity risk-management measures;

f) promoting and developing cybersecurity education and training, skills, awareness-raising and research and development initiatives, as well as guidelines on good practices and controls in cyber hygiene, for citizens, stakeholders and entities;

g) to support academic and research institutions in developing, strengthening and promoting the deployment of cybersecurity tools and secure network infrastructure;

h) including relevant procedures and appropriate information exchange tools to support the voluntary exchange of cybersecurity information between entities, in accordance with European Union law;

i) to strengthen cyber resilience and the cybersecurity hygiene benchmark for small and medium-sized enterprises, in particular those excluded from the scope of this emergency ordinance, by providing easily accessible guidance and assistance for their specific needs;

j) promoting active cyber protection.

Section 2 Competent authority at national level

Article 24

(1) DNSC is the competent authority responsible for cybersecurity and oversight and enforcement tasks for a high common level of cybersecurity.

(2) DNSC performs the function of National Cyber Security Incident Response Team, hereinafter referred to as the National CSIRT, pursuant to the provisions of the Government Emergency Ordinance no. 104/2021.

(3) In order to carry out its duties under the provisions of this emergency ordinance, DNSC ensures that it has sufficient and competent staff and that it has adequate resources to effectively and efficiently perform its duties.

(4) For the application of para. (3), from the DNSC budget, the following categories of expenses is ensured, in compliance with the legal provisions:

a) the purchase of specialised services;

b) procurement of equipment and software, including custom-developed software;

c) affiliation to relevant networks and international organisations and participation through representatives in their work as well as in other relevant events;

d) training and improvement courses, as well as certifications of its own staff;

e) editing publications, specialised guides, awareness videos;

f) organising conferences, seminars and other relevant events;

g) carrying out statistical studies and research activities.

Article 25

(1) DNSC, acting as the competent authority responsible for cybersecurity and with the tasks of supervision and enforcement of the measures for a high common level of cybersecurity pursuant to this emergency ordinance, has the following tasks:

a) develops and ensures the implementation of the national cybersecurity strategy together with the other competent authorities;

b) develops rules and requirements within the scope of this emergency ordinance;

c) develops and updates guidelines, recommendations and best practices within the scope of this emergency ordinance;

d) administers and manages the resources for the implementation of this emergency ordinance;

e) participates, through representatives, in cooperation formats at European level;

f) supervise, verify and control compliance with the provisions of this emergency ordinance;

g) receives complaints about non-compliance by essential and important entities;

h) cooperates with and assists the competent authorities of the other Member States of the European Union, by exchanging information, sending requests and notifications, carrying out control or taking measures to supervise and remedy the deficiencies found, in the case of entities subject to this emergency ordinance;

i) authorizes, revokes or renews the authorization of cybersecurity incident response teams serving essential and important entities;

j) issues, revokes or renews the certificates of cybersecurity auditors who can perform audits within the networks and information systems that support essential services or important services, under the conditions of this emergency ordinance;

k) authorises, revokes or renews the authorisation of cybersecurity training service providers for the training of cybersecurity auditors and cybersecurity incident response teams;

l) ensures the fulfilment of the obligations to report incidents by essential and important entities under the conditions of this emergency ordinance;

m) encourages the use by essential and important entities of ICT products, ICT services and ICT processes that correspond to the cybersecurity standardisation and certification requirements adopted pursuant to art. 49 of Regulation (EU) 2019/881 and of qualified trust services, in compliance with

European and international technical standards and specifications relevant to the security of network and information systems;

n) regulates and manages the process of coordinated disclosure of vulnerabilities.

(2) DNSC is responsible for managing the identification process for essential and important entities and keeps a register of those entities according to art. 18.

(3) DNSC is responsible for managing the identification process of DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines and social media service platforms, and transmits the data to ENISA regarding their identification by January 17, 2025.

(4) DNSC identifies the ICT services, systems and products that may be subject to the national supply chain risk assessment which it prepares and submits to ENISA, with the results of the assessment being transmitted to essential and important entities and sectoral competent authorities.

(5) DNSC keeps track of the data provided for in para. (3), update them regularly and submit the changes to ENISA.

(6) DNSC conducts, whenever necessary and at least once a year, an assessment of the cybersecurity of the national civilian cyberspace, the assessment being also sent to the sectoral competent authorities.

Article 26

(1) DNSC, in the exercise of its supervisory and control tasks, in the event of non-fulfilment by the essential entities and important entities of their obligations according to the provisions of this emergency ordinance, verify compliance with the provisions of this emergency ordinance and carry out controls, issue mandatory provisions for essential entities and important entities in order to comply with and remedy the deficiencies found and sets terms for it establishes supervisory measures for essential entities and important entities and applies sanctions.

(2) DNSC ensures the evaluation of the training and specialization process of auditors for certification as cybersecurity auditors, members of cybersecurity incident response teams, cybersecurity officers and cybersecurity training service providers.

Article 27

(1) DNSC cooperates with the institutions in COSC and may request the performance of security risk checks, including from a national security perspective, on the applicant for an auditor's attestation, members of the cybersecurity incident response teams and service providers specific to the cybersecurity incident response teams.

(2) Following the application of para. (1), DNSC assesses the security risks and, depending on the situation, orders the continuation or interruption of the assessment and certification procedure.

Section 3 National Cyber Crisis Management Framework

Article 28

(1) DNSC is the national authority for cyber crisis management and is responsible for the management of large-scale cybersecurity incidents and cybersecurity crises at national level, a quality that it fulfils through the National Centre for Cyber Security Crisis Management, hereinafter referred to as CNGCSC, according to the provisions of art. 5 letter o) of the Government Emergency Ordinance no. 104/2021.

(2) In fulfilling the quality provided for in para. (1), DNSC has the following tasks:

a) identifies the capabilities, means and procedures that can be used in case of crisis, according to which it develops, updates and coordinates the implementation of the National Peacetime Cyber Security Crisis Management Plan, adopted by order of the Director of DNSC;

b) adopts the technical and organisational measures necessary for the establishment of the critical level of cyber alert and for its management, according to the provisions of Law no. 58/2023;

c) ensures and coordinates the exchange of information related to cybersecurity crises with all relevant public and private sector stakeholders;

d) participates, through CNGCSC, in the coordinated management of large-scale cybersecurity incidents and cybersecurity crises at European Union level and provides support to Member States' authorities;

e) organises and participates, through CNGCSC, in exercises, training activities and other national preparedness measures in the field of cybersecurity crises.

Article 29

(1) The national management of cybersecurity incidents and crises is carried out in accordance with the National Peacetime Cyber Security Crisis Management Plan.

(2) The National Peacetime Cyber Security Crisis Management Plan aims to manage large-scale cybersecurity incidents and cyber crises and includes at least:

a) the objectives of the preparatory measures and activities;

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

c) the cyber crisis management procedures, including their integration into the overall national crisis management framework and information exchange channels;

d) preparedness measures, including exercises and training activities;

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

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

(3) Within three months from the adoption or amendment of the plan provided for in para. (1), DNSC transmits relevant information in relation thereto to the European Commission and the European Network of Cyber Crisis Liaison Organisations, hereinafter referred to as EU-CyCLONe, with the exception of information that may prejudice national security.

(4) Within three months of the entry into force of this emergency ordinance, the National Single Point of Contact notifies the European Commission and EU-CyCLONe of the DNSC's status as a national cyber crisis management authority, as well as any subsequent changes to that status.

Section 4 Cybersecurity incident response teams

Article 30

(1) Essential entities, important entities and sectoral competent authorities may set up cybersecurity incident response teams, hereinafter referred to as CSIRTs, their own or sectoral or may purchase specialised services from CSIRT-specific service providers, authorized by DNSC.

(2) CSIRTs provided for in para. (1) are authorised by DNSC following an assessment of the fulfilment of the specific conditions for the authorisation of this type of service, according to para. (3) and arts. 31 to 33.

(3) In order to obtain authorization, CSIRTs provided for in para. (1) must prove the possession of an adequate, secure and resilient communication and information infrastructure that allows the exchange of information with the entities they serve and with other relevant stakeholders, as well as the existence of adequate resources for the effective performance of their tasks.

(4) CSIRTs provided for in para. 1. cooperate and exchange relevant information with sectoral or cross-sectoral communities of essential entities and important entities, as well as with CSIRTs in third countries, including to provide cybersecurity assistance to them.

(5) CSIRTs provided for in para. (1) participate in national and international cooperation groups, peer reviews, the CSIRT Network or other similar formats at the request of the national CSIRT.

(6) CSIRTs provided for in para. (1) cooperate both with each other and with the national CSIRT.

(7) DNSC may delegate one or more persons from both its own control and specialised staff to temporarily exercise their duties within a CSIRT provided for in para. (1).

Article 31

(1) Their own, sectoral CSIRTs or CSIRT-specific service providers serving essential entities or significant entities have the following obligations:

a) to be authorized by DNSC;

b) ensure the compatibility and interoperability of the systems, procedures and methods used with those of the national CSIRT;

c) to provide at least the minimum package of CSIRT-type services necessary to ensure at national level a unitary protection of essential entities and important entities, under the conditions of para. (2);

d) deploy an appropriate number of qualified persons in the teams;

e) to interconnect with the DNSC alert, monitoring and cooperation service and to ensure a prompt response to the alerts and requests sent by the national CSIRT;

f) have adequate staff to ensure the permanent availability of their services;

g) allocate annually the necessary budget to maintain a high level of capabilities in terms of both human and technical resources.

(2) The technical rules on compatibility and interoperability provided for in para. (1) letter b), the minimum package of CSIRT services referred to in para. (1) letter c) and the criteria for establishing the number of qualified persons provided for in para. (1) letter d) are approved by order of the Director of DNSC.

(3) DNSC elaborates the topics for the specialization of the CSIRTs staff for authorisation according to art. 30 para. (2), by decision of the Director of DNSC.

Article 32

(1) CSIRTs must fulfil the following requirements:

a) ensure high availability of their own communication channels, avoiding single points of failure, having multiple means to be connected and to contact other entities at any time;

b) specify the communication channels provided for in letter a) and make them known to the user base and cooperation partners;

c) to maintain the headquarters and support information systems in secure sites;

d) have an adequate system for handling and routing requests;

e) ensure the confidentiality and credibility of their operations;

f) have adequate staff to ensure the permanent availability of their services;

g) be equipped with redundant systems and backup workspace to ensure the continuity of their services, even after an incident;

h) protect the confidential and sensitive data of the beneficiaries of their services from unauthorised access, theft, alteration or destruction, by means of sufficient, appropriate and proportionate technical and procedural measures.

(2) CSIRTs may prioritise requests for support under a risk-based approach.

(3) CSIRTs establish cooperative relationships with relevant stakeholders in order to carry out their tasks.

(4) In order to facilitate the cooperation provided for in para. (3), CSIRTs promotes the adoption and use of common or standardised practices, classification systems and taxonomies in relation to:

a) incident management procedures;

b) crisis management;

c) coordinated disclosure of vulnerabilities pursuant to art. 36.

(5) The minimum package of CSIRTs must cover at least the medium and high priority functions and controls or elements related to the functions, as defined by internationally recognised standards and frameworks or platforms in the field of incident response and cybersecurity risk-management, to be specified and regularly updated by order of the Director of DNSC.

Article 33

(1) CSIRTs have the following responsibilities:

a) monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, assisting essential entities and important entities involved in real-time or near-real-time monitoring of their network and IT systems in accordance with their needs;

b) ensuring mechanisms for early warning, alerts, announcements and dissemination of information to essential entities and important entities, as well as to competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents in near real-time;

c) responding to incidents and providing assistance to critical entities and important entities involved, as appropriate;

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

e) providing, at the request of a critical entity or a significant entity, a security scan of the networks and information systems of the entity involved to detect vulnerabilities with a potentially significant impact;

f) participating in the implementation of secure information exchange tools, in accordance with art. 20.

(2) The scans provided for in para. (1) letter e) are non-intrusive and are carried out to detect vulnerable or insecurely configured networks and information systems and do not have any negative effect on the functionality of the services of the entities concerned.

Article 34

(1) CSIRTs serving essential entities or important entities are authorised by DNSC.

(2) In this respect, DNSC has the following general tasks:

a) develops and adopts, by order of the Director of DNSC, the regulation on the authorization and verification of CSIRTs serving essential entities and important entities and establishes the conditions of validity for the authorizations granted, as well as the topics for the training of CSIRT staff;

b) grants, extends, suspends or withdraws, by decision of the Director of DNSC, the authorization for CSIRTs;

c) grants, extends, suspends or withdraws, by decision of the Director of DNSC, the authorization of training service providers for CSIRT-specific activities;

d) verify, following referrals or ex officio, whether authorised CSIRTs comply with their obligations.

(3) The authorizations provided for in para. (2) letter b) have a validity of three years.

Article 35

(1) DNSC, as the national CSIRT, can provide incident management support:

a) essential entities and important entities, at their request;

b) cybersecurity incident response teams.

(2) The national CSIRT meets the requirements provided for in art. 30 para. (3) and art. 32 para. (1).

(3) The national CSIRTs may establish cooperation relations with third-country CSIRTs, including to provide them with mutual assistance in cybersecurity matters. In those cooperation relations, an effective, efficient and secure exchange of information with those CSIRTs is facilitated, using the relevant information-sharing protocols.

(4) The national CSIRT may exchange relevant information with third-country CSIRTs, including personal data, in accordance with data protection legislation.

Article 36

(1) DNSC, as the national CSIRT, is responsible for managing the coordinated vulnerability disclosure process and is designated as a coordinator acting as a trusted intermediary, facilitating, where necessary, interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of potentially vulnerable ICT products or ICT services, at the request of any party.

(2) In compliance with the provisions of para. (1), DNSC:

a) ensures the receipt, storage and evaluation of reports regarding any vulnerability of an ICT product or service, submitted under the conditions of para. (3);

b) ensures the possibility of anonymity of the person reporting a vulnerability;

c) identifies and contacts the entities that produce, own or manage ICT products or services that are subject to reporting according to para. (3), to which it communicates the reported vulnerabilities;

d) facilitates, to the extent necessary, when acting as a trusted intermediary, the interaction between the person reporting a vulnerability and the manufacturer, holder, administrator or provider of potentially vulnerable ICT products or services, at the request of one of the parties and with the consent of the other party;

e) orders appropriate measures, in accordance with its legal powers, in relation to the management of vulnerabilities reported by entities that produce, own, manage or provide ICT products or services that are subject to reporting according to para. (3);

f) carry out, where appropriate, checks on vulnerabilities in IT systems, with the support of manufacturers, holders, administrators or providers of potentially vulnerable ICT products or services;

g) negotiates with affected entities timelines for disclosure and management of vulnerabilities affecting multiple entities;

h) when a reported vulnerability could have a significant cross-border impact, cooperates, where appropriate, with the designated CSIRTs within the CSIRT Network;

i) issue procedures, technical standards and guidelines containing minimum requirements and recommendations for vulnerability reporting and whistleblower conduct, their management by entities and their fulfilment of related obligations, private vulnerability disclosure programmes and relations between entities and rapporteurs;

j) can assist people who report a vulnerability.

(3) Any natural or legal person may report vulnerabilities of ICT products or services to DNSC, in compliance with the legal provisions.

(4) Manufacturers and providers of ICT products or services are obliged to submit to DNSC all information on the vulnerabilities they identify as well as on vulnerabilities reported to them by third parties affecting their own products or services and to fix those vulnerabilities within a time limit agreed with DNSC.

(5) The natural or legal person that reports according to para. (3) comply with at least the following:

a) the research activity for the discovery of reported vulnerabilities is carried out in good faith, exclusively for the purpose of contributing to the improvement of cybersecurity and in compliance with the legal provisions;

b) the research activity is carried out without unauthorized access or copying of the content of the files from the computer systems that are the object of the research activity;

c) during the research activity, no data from the computer systems that are the subject of the research activity are deleted or modified;

d) the research activity is carried out without breaching or bypassing technical barriers such as passwords or identification details, through techniques such as brute-force attacks, phishing or other social engineering procedures;

e) no interruption/disruption or damage is caused to third-party ICT products or services;

f) the research activity is not conducted to carry out attacks, does not cause damages and does not use malware or techniques that may affect the availability of ICT services;

g) has not publicly disclosed information on the identified vulnerability, before or after the time of reporting, without the consent of DNSC.

(6) The reporting under para. (3) to be carried out within 48 hours from the identification of the vulnerability.

(7) The entities covered by this emergency ordinance are required to establish at their level ICT vulnerability management processes relating to the products and services they offer and which include at least the following measures:

a) ensures the receipt of vulnerability reports, their analysis in order to confirm or deny the validity of those reported, as well as to remedy the confirmed vulnerabilities, including temporary solutions until they are remedied for the affected persons;

b) cooperation with DNSC in vulnerability management and coordinated vulnerability disclosure processes;

c) establishing and publishing in the technical contact details the ways of contacting and communicating vulnerabilities, as well as the terms and conditions for reporting vulnerabilities in documents and on the website;

d) ensuring communication and cooperation with rapporteurs and DNSC in the process of coordinated disclosure of vulnerabilities, as well as, where appropriate, with users of potentially vulnerable products or services.

Chapter VI Cooperation

Section 1 Cooperation at national level

Article 37

(1) In order to ensure a high common level of cybersecurity at national level, DNSC consults and cooperates with the following:

a) The National Authority for Administration and Regulation in Communications, hereinafter referred to as ANCOM, which is the sectoral competent authority in the field of cybersecurity, according to the provisions of this emergency ordinance, for the sector “8. Digital infrastructure”: “internet exchange point (IXP) providers”, “Data centre service providers”, “Providers of public electronic communications networks” and “Providers of publicly available electronic communications services” in Annex 1 and for sector “1. Postal and courier services" of Annex no. 2;

b) the authorities, as they are identified pursuant to art. 2 para. (2) of Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sectoral rules for cybersecurity aspects of cross-border electricity flows;

c) The Authority for the Digitization of Romania, hereinafter referred to as ADR, which is the sectoral competent authority in the field of cybersecurity, according to the provisions of this emergency ordinance, for the sector "8. Digital infrastructure”: “Trust service providers”;

d) other sectoral competent authorities in the field of cybersecurity, according to Annexes 1 and 2.

(2) In order to ensure a high common level of cybersecurity at national level, DNSC coordinates with CNCPIC and exchanges information on a regular basis for the identification of essential entities identified as critical entities in terms of cyber and non-cyber risks, incidents and threats concerning and affecting them, as well as on the measures taken in response to them.

(3) DNSC cooperates and collaborates with the National Bank of Romania, hereinafter referred to as the BNR, and the Financial Supervisory Authority, hereinafter referred to as ASF, for the assessment and management of cyber risks, the identification of vulnerabilities and the implementation of appropriate protection measures for essential entities and important entities in the banking field and financial market infrastructures, as follows:

a) BNR and ASF transmit to the DNSC information on major ICT-related incidents and significant cyber threats, reported by the entities to which the requirements of the DORA Regulation apply, in a timely manner, and DNSC transmits to the BNR and ASF information on major incidents and cyber threats, reported by the essential or important entities to which this emergency ordinance applies and which have been designated according to the DORA Regulation as suppliers essential ICT services third parties;

b) BNR and ASF may request any type of relevant advice and technical assistance from DNSC, within the limits of the DNSC's capacities and resources, and may establish cooperation agreements to allow for the establishment of effective and rapid coordination mechanisms.

(4) DNSC applies the provisions of art. 3 para. (4) and art. 5 letter h) points 8 and 9 of the Government Emergency Ordinance no. 104/2021.

(5) The sectoral competent authority will be designated by the relevant ministries, by Government decision.

(6) Where an entity operates in two or more sectors, as set out in Annexes 1 and 2, it is subject to proportionate and appropriate technical, operational and organisational measures to manage the risks related to the security of network and information systems at the highest level.

(7) The authorities, as set out in para. (1), may:

a) constitute sectoral CSIRTs, meaning that they monitor, identify, analyse and respond to cybersecurity threats in the corresponding sector and offer preventive, reactive or consultancy public services for cybersecurity management or may purchase specialised services from CSIRT-specific service providers, authorized by DNSC;

b) collect incident reports from its own sector, according to the joint orders provided for in para. (8) letter b);

c) carry out incident investigation activities, under the coordination of the national CSIRT;

d) carry out specific technical activities to identify the vulnerabilities of the networks and information systems of the entities operating in their fields of competence, in which sense it consults and cooperates with the national CSIRT;

e) carry out incident assessment activities in order to identify the main causes, so as to reduce the risk of such incidents;

f) develop cybersecurity guidelines and recommendations within the area of competence to ensure adequate capacity to identify, assess and adopt measures for risk management, cyber incident response and attacks, supply chain security, and crisis management.

(8) The authorities, as set out in para. (1), have the following attributions:

a) transmit to DNSC, to the extent in their possession, cyber threats information and data, including indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools when such exchanges of information and data are aimed at enhancing the digital operational resilience of entities within their remit by raising awareness of cyber threats, limiting or preventing the spread of cyber threats, supporting the range of entities' defensive capabilities, threat detection techniques, mitigation strategies or stages of response and recovery processes;

b) issue joint orders, together with DNSC, in the field of cybersecurity in their area of competence in order to ensure a common high level of cybersecurity at national level, including in relation to the proportionate and appropriate technical, operational and organisational risk-management measures that entities in their field of competence are required to take in the course of their work, the procedure for notification and response to cybersecurity incidents applicable to entities in the field of competence, the specific thresholds and criteria for determining the impact of security incidents in the field of competence;

c) monitors the compliance with the normative acts in the field of cybersecurity, elaborated according to letter b), by the entities in the field of competence and carries out supervision and control activities, according to the provisions of this emergency ordinance, duly applying art. 46 para. (1) and (4)-(9), art. 47 para. (1)-(7), art. 48-50, art. 51 para. (1) and art. 57.

(9) The authorities, as set out in para. (1), have the following obligations:

a) support DNSC in identifying essential entities and important entities in the field of competence according to arts. 5 to 10;

b) participate in the development of the criteria for establishing the impact of incidents, at the request of DNSC;

c) ensure the harmonisation of sector-specific regulations in the field of cybersecurity with the provisions of the regulatory acts issued by DNSC;

d) coordinate with DNSC on the planning and conduct of control activities on cybersecurity issues;

e) submit to DNSC the information relating to infringements of the provisions of this Emergency Order with a view to assisting DNSC in establishing remedial measures and penalties;

(10) Sectoral competent authorities are also empowered to ensure supervision, control and sanctioning in application of the provisions of this emergency ordinance, as well as of the European Union regulations in the field of cybersecurity and the acts implementing the provisions of Directive (EU) 2022/2555 concerning the entities in their sector of competence under this emergency ordinance, where the supervisory, control and sanctioning powers of the Regulations or implementing acts respectively have not been granted to another authority.

(11) The control carried out pursuant to para. (10) is carried out, as the case may be, together with control or specialised personnel from DNSC.

(12) The sectoral competent authorities may exercise their supervisory and control duties provided for by this emergency ordinance, including at the reasoned request of CNCPIC, for the entities identified as critical according to the legal provisions on the resilience of critical entities.

(13) The application of legal acts of the European Union does not derogate from the other obligations incumbent on essential and important entities according to the provisions of this emergency ordinance.

(14) Where sectoral legal acts of the European Union require essential entities or important entities to adopt cybersecurity risk-management measures or to report significant incidents, and those requirements have an effect at least equivalent to the effect of the obligations laid down in this emergency ordinance, the provisions of this emergency ordinance on risk-management measures, incident reporting, as well as supervision, verification and control does not apply to these entities. Where the sectoral legal acts of the European Union do not cover all entities in a given sector falling within the scope of this emergency ordinance, the relevant provisions of this emergency ordinance continue to apply to entities not covered by those sectoral legal acts of the European Union.

(15) The requirements mentioned in para. (14) are considered equivalent in effect to the obligations provided for in this emergency ordinance, if it meets at least one of the following conditions:

a) cybersecurity risk-management measures are at least equivalent in effect to those provided for in art. 13;

b) the sectoral legal act of the European Union provides for immediate access, where appropriate, automatically and directly, to incident reporting for CSIRTs, competent authorities or single points of contact pursuant to this emergency ordinance and if the significant incident reporting requirements have an effect at least equivalent to those provided for in art. 15.

(16) The provisions of para. (7)-(14) do not apply to BNR and ASF.

(17) The joined order provided for in para. (8) letter b) may lay down detailed rules for implementing arts. 11, 13, 15 para. (1), (3), (5) to (10) and art. 16.

(18) DNSC cooperates and collaborates with the Romanian Civil Aviation Authority, hereinafter referred to as AACR, competent authority pursuant to art. 6 para. (1) of Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down detailed rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council as regards the requirements relating to the management of information security risks with a potential impact on aviation security, imposed on organisations covered by Regulations (EU) no. 1321/2014, (EU) no. 965/2012, (EU) no. 1178/2011, (EU) 2015/340 and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, as well as the competent authorities covered by Regulations (EU) no. 748/2012, (EU) no. 1321/2014, (EU) no. 965/2012, (EU) no. 1178/2011, (EU) 2015/340 and (EU) no. 139/2014 and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and amending Regulations (EU) no. 1178/2011, (EU) no. 748/2012, (EU) no. 965/2012, (EU) no. 139/2014, (EU) no. 1321/2014, (EU) 2015/340 and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and art. 5 para. (1) of Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down detailed rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council as regards the requirements relating to the management of information security risks with a potential impact on aviation security imposed on organisations covered by Regulations (EU) no. 748/2012 and (EU) no. 139/2014 of the Commission and amending Regulations (EU) no. 748/2012 and (EU) no. 139/2014 of the Commission, for the assessment and management of cyber risks, the identification of vulnerabilities and the implementation of appropriate protection measures for entities in the field of air transport provided for in Annex no. 1, Transport sector, Air Transport subsector to this emergency ordinance, as follows:

a) AACR and DNSC cooperate in the management of significant cyber incidents and threats reported by the entities under the competence of AACR, and DNSC transmits to the AACR information on cyber incidents and threats, reported by the entities under the competence of AACR and to which this emergency ordinance applies;

b) AACR may request relevant advice and technical assistance from DNSC, within the limits of the DNSC's capacities and resources, and cooperation agreements may be established between the two authorities to allow for the establishment of effective and rapid coordination mechanisms.

(19) DNSC informs the Supervisory Forum established pursuant to art. 32 para. (1) of Regulation (EU) 2022/2554 when exercising its supervisory and supervisory powers to ensure compliance with this emergency ordinance by an essential or important entity, which is designated as a third-party provider of critical ICT services pursuant to art. 31 of Regulation (EU) 2022/2554.

(20) In order to ensure a high common level of cybersecurity at national level in the field of digital transformation and the information society, DNSC cooperates with ADR on cyber risks, incidents and threats.

(21) In order to carry out their duties under the provisions of this emergency Ordinance, the sectoral competent authorities ensure that they have sufficient and competent staff and that they have adequate resources to carry out their duties effectively and efficiently.

Article 38

(1) In the exercise of the duties provided for in art. 37 para. (8) letter b), DNSC and the sectoral competent authority are obliged to comply with the consultation procedure established by this article whenever the measures they intend to adopt are likely to have a significant impact in the field of cybersecurity in the corresponding sector.

(2) DNSC and the sectoral competent authority are obliged to publish the text subject to consultation on their own websites, specifying, at the same time: the date of publication of the document, the date on which the term for submitting comments expires and the estimated date on which they intend to adopt the measure subject to consultation.

(3) From the date on which the text submitted for consultation is published on the websites, DNSC and the sectoral competent authority will grant a period of at least 30 days for the submission of comments, in writing, by any interested person. In situations where it is necessary to adopt emergency measures, DNSC and the sectoral competent authority will grant a period of 10 to 30 days for the submission of observations.

(4) At the latest on the date of publication on the website of the draft order adopting the measure, DNSC and the sectoral competent authority are also obliged to publish a joint summary material with the comments received, in which they will also specify their position on these observations.

(5) DNSC and the sectoral competent authority may decide, by mutual agreement, that only DNSC or only the sectoral competent authority carries out the public consultation procedure. In this case, each authority applies the procedure applicable to its own acts, respecting a permanent dialogue between the two institutions involved.

Article 39

(1) In order to ensure a high common level of cybersecurity at national level, DNSC consults and cooperates with:

a) The Romanian Intelligence Service, for the security of networks and information systems that provide essential services whose impairment is detrimental to national security;

b) The Ministry of National Defence, for the security of networks and information systems that provide essential services in support of national defence activities;

c) The Ministry of Internal Affairs, the National Registry Office for Classified Information, the Foreign Intelligence Service, the Special Telecommunications Service and the Protection and Guard Service, for the security of networks and information systems that provide essential services in their field of activity and responsibility.

(2) DNSC consults and cooperates, as appropriate, with:

a) criminal prosecution bodies;

b) The National Supervisory Authority for the Processing of Personal Data, hereinafter referred to as ANSPDCP, in the case of incidents that result in a breach of personal data security, in accordance with the law.

Section 2 Cooperation at European and international level

Article 40

(1) DNSC serves as single point of contact at national level, in which capacity it facilitates cooperation for the security of networks and information systems with relevant authorities in the Member States, with the European Commission, and with ENISA, including on behalf of other competent authorities in Romania.

(2) As the single point of contact at national level, DNSC has the following attributions:

a) exercises the liaison function between the competent authorities of Romania and the authorities responsible for implementing measures for a high common level of cybersecurity in the Member States, as well as, where appropriate, with the European Commission, ENISA, the Cooperation Group and the CSIRT Network;

b) informs the other Member States or partners affected if the incident has a significant impact on the continuity of essential services or important services in those states;

c) submits summary reports to the Cooperation Group regarding notifications received and actions taken;

d) submits notifications and requests concerning incidents affecting the functioning of essential services in one or more sectors set out in Annexes 1 and 2 to the national authorities or CSIRTs of other Member States, to CSIRTs authorised by DNSC according to the provisions of this emergency ordinance, to the EU-CyCLONe Network, and to the single points of contact in the other Member States, according to their area of responsibility;

e) submits notifications and requests received from other Member States to the competent authorities, according to the area of responsibility;

f) submits to ENISA every three months, a summary report, including anonymised and aggregated data on significant incidents, incidents, significant cyber threats and near misses reported by essential entities and important entities to DNSC, as well as by any other entity, according to arts. 15 and 16.

Article 41

(1) DNSC, as the national CSIRT, participates in the CSIRT Network for operational purposes.

(2) In fulfilling this role, DNSC has the following attributions:

a) participates in the sharing, transfer and exchange of technology among CSIRTs that are part of the Network;

b) participates in the exchange of information on relevant measures, policies, instruments, processes, good practices and frameworks between the CSIRTs that are part of the Network;

c) participates in the exchange of relevant information about incidents, near misses, cyber threats, risks and vulnerabilities;

d) participates in the exchange of information with regard to cybersecurity publications and recommendations;

e) participates in the development of a coordinated Network response to the management of an incident identified within the territory of another Member State;

f) implements and uses the information-sharing specifications and protocols to ensure interoperability with other CSIRTs within the European Union;

g) cooperates with the national CSIRT of a state affected by an incident to facilitate the exchange of information on the incident, cyber threats, risks and vulnerabilities associated with it, at the request of the affected state, member of the Network;

h) supports Member States in addressing cross-border incidents, in accordance with the provisions of Law no. 58/2023;

i) participates in the exchange of best practices and cooperates with other CSIRTs designated as coordinators with regard to the management of the coordinated disclosure of vulnerabilities which could have a significant cross-border impact;

j) takes stock of cybersecurity exercises, including those carried out by ENISA;

k) cooperates and participates in the exchange of information with regional and Union-level Security Operations Centres in order to improve common situational awareness on incidents and cyber threats;

l) evaluates the peer reviews reports, where appropriate;

m) provides guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this emergency ordinance concerning operational cooperation;

n) submits, when applicable, support requests to other members of the Network for the development of a coordinated response of the Network for the management of an incident identified on Romanian territory.

Article 42

In order to facilitate strategic cooperation and information exchange between Member States, DNSC, as the competent authority responsible for cybersecurity and tasked with the supervision and enforcement of measures for a high common level of cybersecurity, participates in the Cooperation Group established at European Union level.

Article 43

DNSC, as CNGCSC, participates in EU-CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and the institutions, organisations, offices and agencies of the European Union.

Article 44

(1) Peer reviews are voluntary and cooperative processes carried out between Member States in which cybersecurity experts, designated by at least two states, different from the Member State being reviewed, assess each other's implementation of cybersecurity measures and operational capacities and involve physical visits or virtual meetings, as well as exchanges of data and information. The Cooperation Group,

in collaboration with the European Commission and ENISA, develops appropriate codes of conduct underpinning the working methods of designated cybersecurity experts.

(2) In accordance with the principle of good cooperation, DNSC provides the designated cybersecurity experts with the information necessary for the assessment, without prejudice to Union or national law concerning the protection of confidential or classified information and to the safeguarding of essential State functions, such as national security.

(3) The peer reviews covers at least one of the following:

a) the level of implementation of the cybersecurity risk-management measures and reporting obligations set out in this emergency ordinance;

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

c) the operational capabilities of CSIRTs;

d) the level of implementation of mutual assistance;

e) the level of implementation of the cybersecurity information-sharing agreements;

f) specific issues of cross-border or cross-sector nature.

(4) DNSC designates cybersecurity experts to carry out the peer reviews based on a methodology that includes objective, non-discriminatory, fair and transparent criteria established by the Cooperation Group.

(5) DNSC ensures that any risk of conflict of interest concerning the designated cybersecurity experts is revealed to the other Member States, the Cooperation Group, the Commission and ENISA, before the commencement of the peer review.

(6) When Romania is subject to peer review, DNSC may object to the designation of particular cybersecurity experts on duly substantiated grounds communicated to the designating Member State. When another Member State is subject to peer review, it may oppose the designation of particular cybersecurity experts under the same conditions as DNSC.

(7) Cybersecurity experts participating in peer reviews draft reports on the findings and conclusions of the peer reviews. The reports include recommendations to enable improvement on the aspects covered by the peer review and are submitted to the Cooperation Group and the CSIRT Network where relevant.

(8) DNSC, when subject to a peer review, may provide comments on the draft reports concerning them and such comments are to be attached to the reports.

(9) DNSC, when subject to peer review, may decide to make its report or an anonymised version of it publicly available.

(10) Before commencing a peer review, DNSC informs the participating Member States of its scope, including the specific aspects provided for in para. (3) letter f).

(11) Prior to the commencement of the peer review, DNSC may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated cybersecurity experts.

(12) Any information obtained through the peer review must be used solely for that purpose. The cybersecurity experts participating in the peer review must not disclose any sensitive or confidential information obtained in the course of that peer review to any third parties.

(13) Once subject to a peer review, the same aspects reviewed in Romania must not be subject to a new peer review for two years following the conclusion of the peer review, unless otherwise decided by DNSC or agreed upon after a proposal of the Cooperation Group.

Article 45

(1) Where an entity registered in Romania as an essential or important entity provides services in more than one Member State, or provides services in one or more Member States and its network and information systems are located in one or more other Member States, DNSC cooperates with the other counterpart competent authorities at European Union level and provide mutual assistance.

(2) In the situation of para. (1), DNSC may request the counterpart competent authorities at the level of the European Union to exercise supervisory and control powers and, where applicable, DNSC may impose fines for the irregularities found by them.

(3) Where an entity provides services in more than one Member State, including Romania, or provides services in one or more Member States, and its network and information systems are located in one or

more other Member States, including Romania, DNSC cooperates with the other counterpart competent authorities at European Union level and provide mutual assistance.

(4) In the situation of para. (3), DNSC may exercise supervisory and control duties at the express request of the counterpart competent authorities at the level of the European Union. Upon receipt of such a request, DNSC may provide mutual assistance to the other authority in proportion to its resources, so that the measures adopted can be implemented in an effective, efficient and consistent manner.

(5) DNSC refuses the request referred to in para. (4), when:

a) it is established that it does not have the competence to provide the requested assistance;

b) the requested assistance exceeds the competences of DNSC according to the legal provisions;

c) the request concerns information or entails activities which, if disclosed or carried out, would be contrary to Romania's interests, respectively in the field of defence, public order and national security.

(6) Before refusing the request referred to in para. (4), DNSC, where applicable, consults the other competent authorities concerned as well as, at the request of one of the Member States concerned, the European Commission and ENISA.

(7) The application of the provisions regarding mutual assistance is carried out in compliance with the provisions of Law no. 58/2023.

Chapter VII Supervision, verification and control

Section 1 Essential entities and important entities

Article 46

(1) In order to ensure compliance with the provisions of this emergency ordinance, as well as with the subsequent normative acts by the entities, DNSC may:

a) carry out supervision, verification and control activities conducted by persons designated for this purpose by a decision of the Director of DNSC;

b) order ad hoc security audits to be carried out by a certified cybersecurity auditor;

c) request the information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to DNSC pursuant to art. 18;

d) request access to data, documents and any information necessary to carry out their supervisory tasks;

e) request data, documents and any information attesting to the implementation of cybersecurity policies, such as the results of cybersecurity audits carried out by a certified auditor and the respective underlying evidence.

(2) The control activity is carried out on the basis of the annual control plan approved by a decision of the Director of DNSC, after its approval by the deputy Director of DNSC who coordinates the regulatory and control activity, or in the following cases, without being limited to them:

a) a significant incident;

b) substantial indications of a breach of the provisions of this emergency ordinance by an entity.

(3) The supervision and control activity is carried out by DNSC, including at the motivated request of CNCPIC, for the entities identified as critical according to the legal provisions on the resilience of critical entities.

(4) In the case of important entities, the supervision according to para. (1) letter a) is carried out only for the implementation of art. 48 para. (2) letters b)-g).

(5) In order to implement para. (1) letter a) with respect to essential entities and important entities, DNSC may perform non-intrusive and proactive cybersecurity scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, with prior notification to the entity concerned and, where appropriate, in cooperation with it.

(6) In order to implement para. (2), DNSC may request access to data, hardware and software equipment, as well as information from the staff of the entities in order to perform its supervisory and control tasks.

(7) On the occasion of conducting the cybersecurity audit under the conditions provided for in art. 11 para. (5) or, as applicable, para. (6), a systematic evaluation of all policies, procedures and protection

measures implemented across certain networks and information systems is carried out, to identify malfunctions and vulnerabilities and recommend measures to remedy them.

(8) No later than 5 days from the completion of any cybersecurity audit, the audited entity submits its results to DNSC and, where applicable, to the sectoral competent authority.

(9) The costs generated by the cybersecurity audit, including the ad hoc one, are borne by the audited entity.

Article 47

(1) In application of the provisions regarding the requests provided for in art. 46 para. (1) letters c)-e), DNSC specifies the purpose and information requested, as well as the term within which the entity must comply, taking into account the urgency of the request.

(2) The findings resulting from the carrying out of the supervision, verification and control activities provided for in art. 46 para. (1) are recorded by the designated control personnel in the findings note.

(3) If the findings note provided for in para. (2) identifies facts that could constitute one of the contraventions referred to in art. 60, the findings note is communicated to the entity concerned in order to submit a position statement on the deficiencies identified, requesting, if necessary, a plan of measures to remedy them.

(4) The position statement provided for in para. (3) is communicated within 3 days from the receipt of the findings note transmitted by DNSC, unless the notified entity requests an extension of the term in order to obtain documentary evidence in support of the position statement, in which case the transmission period may not exceed 10 days.

(5) Within 15 working days from the date of receipt of the findings note according to para. (3) or the transmission of the position statement pursuant to para. (3), as appropriate, the entities are obliged to draw up and submit to DNSC the plan of measures to remedy all the identified deficiencies and the timeframes assumed for their implementation.

(6) The timeframe provided for in para. (5) must be justified in light of the circumstances of the measure by which the deficiency is remedied.

(7) The findings note provided for in para. (2), the position statement referred to in para. (3), as well as the plan of measures provided for in para. (5), when they have been provided, are the basis of the decision of the Director of DNSC by which the contravention is found and the corresponding sanction is ordered.

(8) The application norms and the methodology for risk-based prioritization of supervision, verification and control activities are issued by order of the Director of DNSC.

Article 48

(1) In order to fulfil its duties, as well as to ensure compliance with the provisions of this emergency ordinance by the entities, DNSC applies the following sanctions:

a) warning;

b) contravention fine.

(2) DNSC may order, as appropriate, the following:

a) the adoption of measures when they are necessary to prevent or remedy an incident, as well as time-limits for the implementation of these measures, including an ad hoc audit;

b) the remediation of the deficiencies identified in the application of letter a);

c) the cessation of the entities' conduct by which they violate the provisions of this emergency ordinance;

d) the implementation of the recommendations provided as a result of a security audit;

e) the designation of a person from the control staff with well-defined tasks for a determined period of time, responsible for supervising the compliance of the essential entity concerned with the provisions of arts. 11-14;

f) compliance with cybersecurity risk-management measures provided for in arts. 11-14 and reporting obligations referred to in art. 15, in a certain manner and within a timeframe;

g) breaches of the provisions of this emergency ordinance to be made public by the responsible entity.

(3) When, following the application of the provisions of art. 46 para. (1) letter b), the ad hoc audit reveals the violation of the provisions of this emergency ordinance, it is sanctionable according to para. (1) letter a).

(4) DNSC may order entities to inform, within a specified term, the persons to whom they provide a service or with whom they carry out activities, if they have been or may be affected by a significant cyber threat, of the following:

a) the nature of the threat;

b) the protective or remedial measures that the affected persons may adopt to prevent the occurrence of the significant incident or in order to remedy it.

(5) The measures provided for in para. (1) and (2) are ordered by decision of the Director of DNSC and are communicated to the entity concerned within 60 days from the issuance of the decision.

Article 49

(1) When the measures provided for in art. 48 are not sufficient to determine if the essential entities complied with the requests to remedy the deficiencies within a reasonable timeframe, by decision of the Director of DNSC, the following may be ordered:

a) notification of sector-specific competent authorities, institutions or entities with a view to temporarily suspend the certification or authorisation issued for the entity concerned, for part or all of the relevant services provided, or for the relevant activities carried out by that entity;

b) notification of the competent authorities, institutions or entities to impose a temporary ban on exercising the management function at the level of executive director or legal representative in the entity concerned.

(2) The suspension and temporary prohibition imposed pursuant to para. (1) apply until DNSC notifies the competent authorities, institutions or entities according to para. (1) of the termination of the cause for which they were ordered.

(3) The measures provided for in para. (1) do not apply to public administration entities falling within the scope of this emergency ordinance.

Article 50

(1) The establishment of the measures provided for in arts. 48 and 49, is to be carried out by assessing, at least:

a) the duration of the act;

b) the existence of a previous infringement;

c) the material or non-material damages caused by the act;

d) the measures adopted by the entity in order to prevent or remedy the effects of the act;

e) the entity's conduct in relation to the certification mechanisms to which it has adhered or the codes of conduct assumed;

f) the conduct of responsible persons in relation to the competent authorities.

(2) The following acts constitute serious violations:

a) repeated violations;

b) failure to notify or remedy significant incidents;

c) failure to comply with the obligation to remedy the deficiencies found by the competent authorities;

d) obstruction of audits or monitoring activities ordered by DNSC following the findings;

e) providing false or grossly inaccurate information in relation to cybersecurity risk-management measures provided for in arts. 11-14 or reporting obligations referred to in art. 15;

f) restricting the access of the personnel designated for this purpose by DNSC in the spaces subject to control, as well as to the data and information necessary for the control;

g) non-compliance with the provisions issued by DNSC pursuant to art. 48 para. (2).

(3) The entity's management bodies are responsible for allowing the access of the personnel, designated for this purpose by DNSC, to the spaces subject to control, as well as to the data and information necessary for the control.

(4) The general meeting of shareholders is not the governing body of essential and important entities within the meaning of this emergency ordinance.

Article 51

(1) DNSC or, as appropriate, the sectoral competent authority informs CNCPIC when exercising its supervisory and control powers over an essential entity identified as a critical entity in accordance with the legal provisions on the resilience of critical entities.

(2) CNCPIC may request DNSC to exercise its supervisory and control powers over an essential entity identified as a critical entity in accordance with the legal provisions on the resilience of critical entities.

Article 52

DNSC may propose the empowerment by Government decision of other sectoral competent authorities in the field of cybersecurity for the corresponding field of competence in order to fulfil the duties provided for in arts. 46-51 and arts. 60-63.

Section 2 CSIRTs, auditors and cybersecurity training service providers

Article 53

(1) DNSC supervises, verifies and controls the activity of the CSIRTs of essential entities and important entities or sectoral CSIRTs, CSIRT-specific service providers, as well as cybersecurity auditors, when they provide specialised services to essential entities and important entities.

(2) DNSC, in the exercise of the supervisory, verification and control attributions, in case of non-fulfilment of obligations by the CSIRTs of essential entities and important entities or sectoral CSIRTs, the providers of CSIRT-specific services, as well as the cybersecurity auditors, carries out control activities in order to verify the fulfilment of the obligations, requirements and responsibilities provided for in arts. 31-33, issues binding provisions to comply with and remedy the deficiencies found and sets terms for compliance, establishes supervisory measures and imposes sanctions.

Article 54

(1) DNSC supervises, verifies and controls the activity of cybersecurity training service providers for auditors and CSIRTs.

(2) DNSC, in the exercise of its supervisory, verification and control attributions, in case of non-fulfilment of obligations by the providers of cybersecurity training services for auditors and CSIRTs, carries out control activities in order to verify the fulfilment of the provisions of the order from para. (3), issues mandatory provisions in order to comply with and remedy the deficiencies found and establishes terms for their compliance, establishes supervisory measures and applies sanctions.

(3) DNSC develops the regulation on the authorisation, verification and revocation of cybersecurity training service providers for auditors and CSIRTs and establishes the conditions of validity for the authorisations granted to them by order of the Director of DNSC.

Article 55

(1) If, as a result of the verifications, serious violations are found, DNSC may order the suspension of the cybersecurity auditors' certificate or the authorization of the CSIRTs for a determined period of time, in order to remedy them, or, as appropriate, their withdrawal.

(2) Annually, by March 31, cybersecurity auditors submit to DNSC, in electronic format, a statement of the security audits carried out in the previous calendar year, namely the number, beneficiaries, periods, serious irregularities found and vulnerabilities found.

Article 56

(1) DNSC supervises, verifies and controls compliance with the provisions of this emergency ordinance with regard to the obligations arising from the authorisation and attestation activities for the CSIRTs of essential entities and important entities or sectoral CSIRTs, CSIRTs specific service providers, as well as cybersecurity auditors.

(2) The rules for the application of the provisions on supervision, verification and control for the CSIRTs of the essential entities and important entities or sectoral CSIRTs, the CSIRT-specific service providers, as well as the cybersecurity auditors are approved by order of the Director of DNSC.

(3) The authorization, suspension and withdrawal of authorisation, as well as the reauthorisation of cybersecurity training service providers for auditors and CSIRTs are ordered by decision of the Director of DNSC.

(4) The cybersecurity training service provider authorisation for auditors and CSIRTs is issued by DNSC based on the evaluation criteria, with a limited validity of four years.

Chapter VIII Cybersecurity audit

Article 57

(1) The cybersecurity audit can be:

a) periodical, takes place on a regular basis, according to the order in art. 11 para. (5) or, as appropriate, para. (6);

b) ad hoc, based on the decision of the Director of DNSC according to para. (2).

(2) The ad hoc cybersecurity audit is exceptional in nature and represents the audit activity carried out by an auditor certified according to the provisions of this emergency ordinance, regarding an essential entity or an important entity, at the reasoned request of DNSC, as a result of:

a) a significant incident;

b) a change which has significant impact on networks and information systems, but no later than 180 days after its occurrence;

c) substantiated indications of a breach of the provisions of this emergency ordinance by an essential entity.

(3) When an ad hoc audit is ordered, DNSC communicates to the entity both the reasons and the objectives of the audit.

(4) The audited entity has the right to select the auditor.

(5) The change with a significant impact on the networks and information systems provided for in para. (2) letter b) is generated by:

a) the introduction of a new network or information system involved in the provision of the service;

b) the introduction of new technology for the provision of the service;

c) a change in the mode of operation of the service;

d) a change in the quality of the entity, from an important entity to an essential entity.

(6) The substantial indications referred to in para. (2) letter c) may result from the control measure carried out by DNSC personnel, the information received from the authorities referred to in art. 10 of Law no. 58/2023, CNCPIC, the sectoral competent authorities provided for in art. 37, as well as from other entities according to art. 25 of Law no. 58/2023 or as a result of the analyses of the incidents reported through the incident reporting platform.

(7) During the periodic cybersecurity audit, a systematic evaluation of all policies, procedures and protection measures implemented at the level of some networks and information systems is carried out, in order to identify malfunctions and vulnerabilities and recommend measures to remedy them.

(8) In a maximum of 15 working days from the date of receipt of the audit report, the entities are obliged to prepare and submit to DNSC and, as appropriate, to the sectoral competent authority, based on the recommendations issued by the auditor, the plan of measures to remedy all the deficiencies found and the timeframes assumed for their implementation.

(9) The entities are obliged to implement the plan of measures provided for in para. (8) within the assumed timeframe.

(10) The concerned entity notifies DNSC and, where applicable, the sectoral competent authority regarding the implementation of all the measures provided for in para. (8), and provides supporting documents in this regard, in a maximum of five days from the expiry of the assumed deadline.

(11) The terms provided for in para. (9) must be justified in light of the circumstance of the measure by which the deficiency is remedied.

Article 58

(1) The cybersecurity audit is carried out by the cybersecurity auditors who hold a valid certificate issued by DNSC, except for the cybersecurity audit carried out at the level of the institutions with responsibilities in the field of defence, public order and national security, as well as for the services made available by them.

(2) In this regard, DNSC:

a) keeps the record of cybersecurity auditors;

b) develops the regulation on the certification and verification of cybersecurity auditors and establishes the conditions of validity for the certificates granted to them by order of the Director of DNSC;

c) grants, extends, suspends or withdraws the cybersecurity auditors' certificate, according to the regulation provided for at letter b);

d) verifies, following the notifications or ex officio, the fulfilment by certified auditors of their legal obligations;

e) develops the themes for the specialization of auditors for the attestation provided for in letter c), by decision of the Director of DNSC.

(3) The following cannot perform a cybersecurity audit:

a) certified auditors who routinely provide cybersecurity or CSIRT-type services to the essential entities or important entities concerned or are employees thereof;

b) the auditor who has a service contract for the audited network or system in progress at the time the audit is carried out or within a period of less than one year;

c) the auditor who has carried out 3 consecutive audits at the same essential entity or significant entity.

(4) The audit activity is carried out according to the European and international standards and specifications applicable in the field.

(5) The audit topics will take into account the technical rules in force on the security of the networks and information systems of essential entities and important entities, developed under this emergency ordinance.

(6) The certificates are valid for 3 years.

(7) The list of European and international standards and specifications provided for in the provisions of para. (4) is established and approved by decision of the Director of DNSC, which updates whenever necessary.

(8) In carrying out a security audit activity, the cybersecurity auditor must:

a) demonstrate professional integrity, acting honestly and fairly in all professional engagements, providing true and accurate assessments;

b) to comply with the codes of ethics issued by DNSC and the Body of Information Systems Auditors of Romania, to demonstrate and maintain transparency in communication;

c) not be in a conflict of interest that could affect their independence, whether of a financial, personal or professional nature, in order to be able to make decisions independently and without any influence from the audited entity or other stakeholders;

d) protect the confidentiality of information obtained during the audit process, meaning that they must ensure that access to sensitive information is restricted only to authorised personnel and that this information is stored securely, in accordance with the relevant regulations governing audit practices, including those specific to cybersecurity.

Article 59

(1) For the purpose of granting and withdrawing the certification of cybersecurity auditors, as well as for the organisation and coordination of cybersecurity audit activities, the Body of Information Systems Auditors of Romania is established by Government decision drafted by DNSC, within two years from the entry into force of this emergency ordinance.

(2) The Body of Information Systems Auditors of Romania is organised and operates as a non-profit public utility professional organisation with legal personality, under the coordination of DNSC.

(3) The main objective of the Body of Information Systems Auditors of Romania is to regulate standards, as well as the Code of Ethics for the professional practice of cybersecurity auditing, and to continuously monitor information systems auditing activities in Romania.

(4) The organisational structure of the Body of Information Systems Auditors of Romania is to be approved by order of the Director of DNSC.

(5) DNSC coordinates the drafting of regulations for organisation, operation, and internal rules.

(6) The Body of Information Systems Auditors of Romania may have in its structure subunits with or without legal personality, departments, sections and may acquire the quality of associate or founding shareholder within other commercial companies or organisational structures necessary for the achievement of its object of activity.

Chapter IX Penalties

Article 60

(1) The following acts constitute contraventions if they were not committed under such conditions as to be considered offenses according to the law:

a) non-compliance by essential and important entities with the obligation to take technical, operational and organisational measures provided for in art. 11 para. (1) under the conditions and in compliance with the imposed requirements;

b) non-compliance by essential and important entities with the obligation to undergo a cybersecurity audit according to the conditions established in art. 11 para. (5) or, as appropriate, para. (6), within the indicated term;

c) non-compliance by essential and important entities with the obligation to transmit the required data according to art. 11 para. (7) within the term and under the conditions set out in the application;

d) non-compliance by essential and important entities with the obligation to transmit the required data according to art. 11 para. (9) within the term and under the conditions set out in the application;

e) non-compliance by essential and important entities with the obligation to annually carry out and submit maturity level self-assessment according to art. 12 para. (4);

f) non-compliance by essential entities with the obligation to prepare and submit the plan of measures to remedy the deficiencies according to art. 12 para. (5), within 30 days from the completion of the self-assessment;

g) non-compliance by members of the management bodies of essential and important entities with the obligation to supervise the implementation of risk-management measures according to art. 14 para. (1);

h) non-compliance by members of the management bodies of essential and important entities with the obligation to attend professional training courses in the field of cybersecurity according to art. 14 para. (2);

i) non-compliance by members of the management bodies of essential and important entities with the obligation to establish the permanent means of contact according to art. 14 para. (3);

j) non-compliance by members of the management bodies of essential and important entities with the obligation to allocate resources according to art. 14 para. (3);

k) non-compliance by members of the management bodies of essential and important entities with the obligation to designate those responsible for the security of networks and information systems according to art. 14 para. (3);

l) non-compliance by essential and important entities with the reporting obligation pursuant to art. 15 para. (1) in compliance with the terms and conditions established according to art. 15;

m) non-compliance by essential and important entities with the obligation to notify the recipients of the services in compliance with the terms and conditions established according to art. 15 para. (1);

n) non-compliance by essential and important entities with the obligation to report information in compliance with the terms and conditions established according to art. 15 para. (3);

o) non-compliance by entities in the sectors provided in Annexes no. 1 and 2 with the obligation to notify according to art. 18 para. (2) within the indicated term;

p) non-compliance by entities in the sectors provided in Annexes no. 1 and 2 with the obligation to provide information according to art. 18 para. (3) within the indicated term;

q) non-compliance by essential and important entities with the obligation to transmit the risk level assessment according to art. 18 para. (6) within the indicated term;

r) non-compliance by essential and important entities with the obligation to self-assess the maturity level according to art. 18 para. (7) within the indicated term;

s) non-compliance by essential and important entities with the obligation to communicate the amendments according to art. 18 para. (8) within the indicated terms;

t) non-compliance by essential and important entities with the obligation to notify according to art. 18 para. (13) within the indicated term;

u) non-compliance by TLD name registries and entities providing domain name registration services with the obligation to collect data according to art. 19 para. (1);

v) non-compliance by TLD name registries and entities providing domain name registration services with the obligation to establish policies and procedures according to art. 19 para. (3);

w) non-compliance by TLD name registries and entities providing domain name registration services with the obligation to make data available to the public according to art. 19 para. (4);

x) non-compliance by TLD name registries and entities providing domain name registration services with the obligation to provide access to data according to art. 19 para. (8);

y) non-compliance by TLD name registries and entities providing domain name registration services with the obligation to make publicly available the policies and procedures regarding data disclosure according to art. 19 para. (9);

z) non-compliance by TLD name registries and entities providing domain name registration services with the obligation to respond to access requests according to art. 19 para. (9);

aa) carrying out activities specific to CSIRT teams, by entities that do not have that authorization according to art. 34;

bb) non-compliance by manufacturers and suppliers of ICT products or services with the obligation to transmit information according to art. 36 para. (4);

cc) non-compliance by manufacturers and suppliers of ICT products or services with the obligation to remedy vulnerabilities according to art. 36 para. (4) within the mutually agreed term;

dd) non-compliance by essential and important entities with the obligation to establish vulnerability management processes according to art. 36 para. (7);

ee) non-compliance by essential and important entities with the obligation to transmit audit results according to art. 46 para. (8), within the indicated term;

ff) non-compliance by essential and important entities with the obligation to inform when it was ordered as such by DNSC according to art. 48 para. (4), within the indicated period;

gg) non-compliance by CSIRTs of essential entities and important entities, sectoral CSIRTs, CSIRT-specific service providers and cybersecurity auditors with the provisions issued by DNSC according to art. 53 para. (2), within the indicated terms;

hh) non-compliance by providers of cybersecurity training services for auditors and CSIRTs with the provisions issued by DNSC according to art. 54 para. (2), within the indicated terms;

ii) non-compliance by cybersecurity auditors with the obligation to transmit information according to art. 55 para. (2), within 30 days from the completion of the term granted;

jj) non-compliance by essential and important entities with the obligation to draw up and transmit the plan of measures according to art. 57 para. (8), within the indicated term;

kk) non-compliance by essential and important entities with the implementation obligation according to art. 57 para. (9), within the assumed term;

ll) non-compliance by essential and important entities with the obligation to notify and make available the supporting documents according to art. 57 para. (10), within the indicated term;

mm) non-compliance of essential and important entities with the obligation to comply with the modalities for implementing the provisions of art. 11 para. (2), (4), (8) and (10), art. 13, art. 15 para. (1), (3), (5)-(10) and art. 16 established by joint orders issued in accordance with the provisions of art. 37;

nn) non-compliance by essential and important entities with the obligation to submit to DNSC or, as appropriate, to the sectoral competent authority, the information requested pursuant to art. 46 para. (1) letter c)-e);

oo) non-compliance by essential and important with the obligation to prepare and submit to DNSC or, as appropriate, to the sectoral competent authority, the plan of measures to remedy all the deficiencies found and the terms assumed for their implementation, according to art. 47 para. (5).

(2) By derogation from the provisions of art. 8 para. (2) letter a) of Government Ordinance no. 2/2001 on the legal regime of contraventions, approved with amendments and completions by Law no. 180/2002, as subsequently amended and supplemented, the contraventions provided for in para. 1 are sanctioned as follows:

a) for important entities, a fine from 5,000 lei to a maximum of the equivalent in lei of 7,000,000 euros, or no more than 1.4% of the net turnover, whichever is higher, for the contraventions provided for in para. (1) letters a)-d), f)-m), dd), jj) and mm);

b) for essential entities, a fine from 10,000 lei to a maximum of the equivalent in lei of 10,000,000 euros or no more than 2% of the net turnover, whichever is higher, for the contraventions provided for in para. (1) letters a)-m), dd), jj) and mm);

c) for important entities, a fine from 1,000 lei to 300,000 lei for the contraventions provided for in para. (1) letters n)-t), ee)-ff), kk)-ll) and nn)-oo);

d) for essential entities, a fine from 1,500 lei to 500,000 lei, in the case of para. (1) letters n)-t), ee)-ff), kk)-ll) and nn)-oo);

e) fine from 1,000 lei to 100,000 lei, for the contraventions provided for in para. (1) letters u)-z), aa)-cc) and gg)-ii).

(3) The net turnover provided for in para. (2) letters a) and b) is the one registered by the important or essential entity in the last financial year.

(4) In order to individualize the sanction provided for in para. (2), the criteria referred to in art. 50 para. (1) are taken into account, and when the provisions of art. 50 para. (2) are applicable, the amount of the fine may be set up to double the limits provided for in para. (2).

(5) For newly established legal entities and for legal entities that did not register the turnover in the financial year prior to the sanction, the fine provided for in para. (2) is set at an amount between a minimum of one and a maximum of 50 gross national minimum wages.

(6) To the extent that this emergency ordinance does not provide otherwise, the contraventions provided for in para. (1) are subject to the provisions of Government Ordinance no. 2/2001.

(7) By derogation from the provisions of art. 16 para. (1), art. 28 para. (1) and art. 29 of Government Ordinance no. 2/2001, in the case of sanctions applied for committing the contraventions provided for in para. (1), the offender may, within a maximum of 15 days from the date of delivery or communication of the act of finding the contravention and applying the sanction, pay half of the amount of the fine imposed, the ascertaining agent mentioning this possibility in the report, the mention also being included in the decision by which the sanction is applied.

Article 61

(1) The finding of the contraventions provided for in art. 60 para. (1) are carried out according to the provisions of art. 46-50.

(2) The finding of the contraventions provided for in art. 60 para. (1) letters a)-n), ee), ff), jj)-oo) is carried out by DNSC or by the control staff of the sectoral competent authorities according to art. 37 para. (1), for the essential or important entities, as appropriate, which carry out their activity in the field of competence of these authorities, the application of the sanction being carried out, in the case of the sectoral competent authorities, by decision of their management, with the corresponding application of para. (3)-(8). The finding of the contraventions referred to in art. 60 para. (1) letters o)-dd), gg)-ii) is carried out by DNSC, the application of the sanction being carried out by decision of the Director of DNSC.

(3) The decision of the Director of DNSC to ascertain the contravention and to apply the sanction includes the following:

a) the identification data of the contravener;

b) the date when the act was committed;

c) description of the contravention and the circumstances that were taken into account when individualizing the sanction;

d) indication of the legal basis according to which the contravention is established and sanctioned;

e) the sanction applied;

f) the term and method of payment of the fine, in case of application of the fine as a sanction;

g) the term for exercising the appeal and the competent court.

(4) By derogation from the provisions of art. 13 of the Government Ordinance no. 2/2001, the application of the sanction set out in this emergency ordinance is prescribed within three years from the date of the commission of the act. In the case of infringements that last over time or those consisting of committing,

on the basis of the same resolution, at different intervals of time, several actions or inactions, each of which constitutes the content of the same contravention, the prescription begins to run from the date of the finding, or from the date of cessation of the last act or fact committed, if this moment occurs prior to the finding.

(5) The offender is also notified of the payment notice, which contains the mention regarding the obligation to pay the fine within 30 days from the date of communication of the document.

(6) If the decision to ascertain the contravention and to apply the sanction provided for in para. (2) is not challenged within the term referred to in para. (8), along with the final court decision by which the administrative action was resolved, constitute an enforceable title, without any other formality. The action in administrative litigation under the conditions provided for in para. (8) suspends the execution only with regard to the payment of the fine, until the court pronounces a final decision.

(7) The amounts derived from the fines imposed in accordance with the provisions of this article are paid in full to the state budget. The execution is carried out in accordance with the legal provisions on the enforcement of tax claims. In order to enforce the sanction, DNSC and the sectoral competent authorities provided for in art. 37, communicate, ex officio, to the specialised bodies of the National Agency for Fiscal Administration the decision to ascertain the contravention and to apply the sanction referred to in para. (2) or (3), not challenged within the term provided for in para. (8), after the expiry of the term provided in the payment notice or after the court decision by which the administrative action was resolved has become final.

(8) By way of derogation from the provisions of art. 7 of the Law on Administrative Litigation no. 554/2004, as subsequently amended and supplemented, and from the provisions of art. 32 para. (1) of Government Ordinance no. 2/2001, the administrative acts, decisions and decisions establishing the contravention and applying the sanction adopted according to the provisions of this emergency ordinance may be appealed in administrative proceedings to the Bucharest Court of Appeal, without going through the prior procedure, within 30 days from their communication.

Article 62

(1) DNSC informs, without undue delay, ANSPDCP when, in the exercise of its supervisory and control powers according to the provisions of this emergency ordinance, it finds aspects specific to cybersecurity policies or incidents that may have an impact on the protection of personal data.

(2) DNSC does not apply the provisions of art. 48 para. (1) for facts with an impact in the field of personal data protection in respect of which an investigation has been carried out or is being carried out by ANSPDCP.

(3) The processing of personal data falling under the scope of this emergency ordinance is carried out in compliance with the legal regulations on the protection of natural persons with regard to the processing of personal data.

(4) The reports made pursuant to this emergency ordinance does not affect the obligations of personal data controllers established pursuant to arts. 33 and 34 of Regulation (EU) 2016/679.

(5) Where the competent supervisory authority under Regulation (EU) 2016/679 is established in another Member State, DNSC informs ANSPDCP of the potential data breach according to para. (1).

Article 63

DNSC informs the institutions with attributions in the coordination of the activity and control in the field of protection of classified information as established by Law no. 182/2002 on the protection of classified information, with subsequent amendments and completions, and subsequent normative acts if it is found that cybersecurity incidents may have an impact on the protection of restricted or state secret data and information.

Chapter X Transitional and final provisions

Article 64

(1) The measures adopted or imposed by ANCOM pursuant to the provisions of Chapter IV of the Government Emergency Ordinance no. 111/2011, by Decision no. 70/2024 of the President of ANCOM on the security of public electronic communications networks and electronic communications services intended for the public, remain in force until their revision.

(2) The provisions of this emergency ordinance apply to all acts and facts concluded or, as appropriate, produced or committed after its entry into force, as well as to legal situations arising after its entry into force.

(3) Subsequent acts adopted pursuant to this emergency ordinance produce legal effects to the extent that they do not contravene the legal regulations in force.

(4) The provisions of arts. 60 and 61 enter into force 30 days after the date of publication of this emergency ordinance in the Official Gazette of Romania, Part I.

Article 65

(1) By order of the Director of DNSC, published in the Official Gazette of Romania, Part I, the following are approved:

a) the criteria and thresholds for determining the degree of disruption of a service and the methodology for assessing the level of risk of entities, pursuant to art. 10 para. (2), within 20 days from the date of entry into force of this emergency ordinance;

b) risk-management measures, pursuant to art. 12 para. (1), within 120 days from the date of entry into force of this emergency ordinance;

c) the methodological norms regarding the reporting of incidents, pursuant to art. 15 para. (17), within 120 days from the date of entry into force of this emergency ordinance;

d) the requirements regarding the notification process for registration and the method of transmission of information, pursuant to art. 18 para. (9), within 15 days from the date of entry into force of this emergency ordinance;

e) the National Peacetime Cyber Security Crisis Management Plan, pursuant to art. 28 para. (2), within 180 days from the date of entry into force of this emergency ordinance;

f) the technical norms regarding the compatibility and interoperability of the systems, procedures and methods used by CSIRTs and the criteria for establishing the number of qualified persons, pursuant to art. 31 para. (2), within 120 days from the date of entry into force of this emergency ordinance;

g) the minimum package of CSIRT services, pursuant to art. 32 para. (5), within 120 days from the date of entry into force of this emergency ordinance;

h) the regulation on the authorization and verification of CSIRTs, the conditions of validity for the authorizations granted and the topics for the training of CSIRT personnel, pursuant to art. 34 para. (2) letter a), within 120 days from the date of entry into force of this emergency ordinance;

i) the rules of application and the methodology for risk-based prioritization of supervision, verification and control activities, pursuant to art. 47 para. (8), within 120 days from the date of entry into force of this emergency ordinance;

j) the regulation on the authorization, verification and revocation of cybersecurity training service providers for auditors and CSIRTs and the conditions of validity for the authorizations granted to them, pursuant to art. 54 para. (3), within 120 days from the date of entry into force of this emergency ordinance;

k) the rules for the application of the provisions on supervision, verification and control for CSIRTs, CSIRT-specific service providers, as well as for cybersecurity auditors, pursuant to art. 56 para. (2), within 120 days from the date of entry into force of this emergency ordinance;

l) the regulation on the certification and verification of cybersecurity auditors and the conditions of validity for the certificates granted, pursuant to art. 58 para. (2) letter b), within 120 days from the date of entry into force of this emergency ordinance.

(2) By decision of the Director of DNSC, published in the Official Gazette of Romania, Part I, the following are approved:

a) the topics for the specialization of auditors in view of certification, pursuant to art. 58 para. (2) letter e), within 180 days from the date of entry into force of this emergency ordinance;

b) the topics for the specialization of CSIRTs' personnel in view of authorization, pursuant to art. 31 para. (3), within 180 days from the date of entry into force of this emergency ordinance.

Article 66

(1) On the date of entry into force of this emergency ordinance, the following are repealed:

a) Law no. 362/2018 on ensuring a high common level of security of networks and information systems, published in the Official Gazette of Romania, Part I, no. 21 of 9 January 2019, with the exception of measures adopted or imposed pursuant to the provisions of Chapters IV and V, which remain in force until their revision, according to art. 65;

b) Art. 4 para. (1) points 54^1 and 54^2, as well as Chapter IV: Security of electronic communications networks and services of the Government Emergency Ordinance no. 111/2011;

c) Law no. 146/2014 on the authorisation of the payment of dues to the International Forum of Incident Response and Security Teams (FIRST) and to the TF/CSIRT Trusted Introducer (TI) Forum of the Trans-European Research and Education Networking Association (TERENA) in order to maintain the participation of the National Computer Emergency Response Team CERT-RO to these two non-governmental bodies, with subsequent amendments and completions.

(2) The references made by other normative acts to Law no. 362/2018 on ensuring a high common level of security of networks and information systems are considered to be made to this emergency ordinance.

Article 67

(1) Until December 31, 2027, in order to obtain an adequate level of qualified personnel, for the positions that according to the job description contribute to the fulfilment of the duties provided for by this emergency ordinance, DNSC, AACR, ANCOM and other authorities with sectoral competences do not apply the provisions of:

a) art. VII of the Government Emergency Ordinance no. 115/2023 on some fiscal-budgetary measures in the field of public spending, for fiscal consolidation, combating tax evasion, for amending and supplementing certain normative acts, as well as for the extension of certain terms, with subsequent amendments and completions, as well as the provisions of general normative acts aimed at restrictions on the occupation by competition or examination of vacant or temporarily vacant positions in the budgetary sector;

b) art. XVII para. (7) or, as appropriate, art. XXXII of Law no. 296/2023 on some fiscal-budgetary measures to ensure Romania's long-term financial sustainability, as subsequently amended and supplemented.

(2) By derogation from the provisions of art. III of the Government Emergency Ordinance no. 1/2020 on some fiscal-budgetary measures and for the amendment and completion of certain normative acts, with subsequent amendments and completions, until December 31, 2027, in order to obtain an adequate level of qualified personnel, for the positions that according to the job description contribute to the fulfilment of the duties provided by this emergency ordinance, the occupation by secondment of vacant or temporarily vacant positions within ANCOM and other authorities with competences at national level will be carried out exclusively under the conditions of Law no. 53/2003 - Labor Code, republished, with subsequent amendments and completions.

(3) In order to obtain an adequate level of qualified personnel, until December 31, 2027, the filling by competition of the vacant and temporarily vacant positions provided for in para. (1)-(2) is carried out exclusively under the conditions of Law no. 53/2003 – Labor Code, republished, with subsequent amendments and completions, of the Government Emergency Ordinance no. 57/2019 on the Administrative Code, with subsequent amendments and completions, as appropriate, and of the normative acts specific to each authority.

(4) By way of derogation from art. 47 para. (2) of Law no. 53/2003, republished, with subsequent amendments and completions, in the case of personnel who are not compensated under Law no. 153/2017 on the remuneration of personnel paid from public funds, the rights due to the seconded employee may not exceed the level of rights that the staff of the public authority or institution to which he is posted may benefit. If the salary rights from the employer who ordered the secondment are more favourable, the employee can refuse the posting.

(5) In the application, as appropriate, of the provisions of para. (2), by derogation from the provisions of art. 505 para. (2) of the Government Emergency Ordinance no. 57/2019 on the Administrative Code, as subsequently amended and supplemented, the occupation by secondment of vacant or temporarily vacant contractual positions may be carried out including with personnel with the status of civil servant or civil servant with special status. The secondment is carried out with the prior notification of the National Agency of Civil Servants according to the provisions of art. 505 para. (6) and (7) of the Government Emergency Ordinance no. 57/2019, as subsequently amended and supplemented.

(6) The secondment provided for in para. (5) is ordered for a fixed period, under the conditions referred to in art. 46 para. (1) and (2) of Law no. 53/2003, republished, with subsequent amendments and completions, only with the written consent of the civil servant or of the civil servant with special status to be seconded, in compliance with the provisions of art. 505 para. (8) of the Government Emergency Ordinance no. 57/2019, as subsequently amended and supplemented, at least 10 days before the measure is ordered.

(7) By derogation from the provisions of art. 505 para. (3) and (5) of the Government Emergency Ordinance no. 57/2019, as subsequently amended and supplemented, the secondment under the conditions of para. (5), from a public executive or management function to a contractual executive or management position, if the civil servant or civil servant with special status meets the employment conditions provided in the job description of the contractual position to which he is seconded.

(8) During the secondment under the conditions of para. (5), the civil servant or the civil servant with special status benefits from the more favourable salary rights, respectively either the rights corresponding to the public function from which he was seconded, or to the contractual position to which he was seconded.

(9) The period for which the secondment was ordered under the conditions of this article is considered seniority in the civil service, respectively in the public service with special status, as appropriate, as well as seniority in the specialty of studies.

(10) For executive civil servants, the period of secondment under the conditions of this article is considered seniority in the professional grade of the civil service from which they are seconded and is taken into account for promotion.

(11) By derogation from the provisions of art. 94 para. (2) letter a) of Law no. 161/2003 on some measures to ensure transparency in the exercise of public dignities, public functions and in the business environment, prevention and sanctioning of corruption, with subsequent amendments and completions, the secondment of civil servants and civil servants with special status, under the conditions of this article, does not represent a situation of incompatibility.

(12) The secondment of civil servants with special status - police officers is carried out under the conditions of Law no. 360/2002 on the Policeman's Statute, with subsequent amendments and completions. The secondment may be ordered, with the written consent of the civil servant with special status - policeman, for a period of no more than one year.

Exceptionally, the period of secondment may be extended for objective reasons that require the presence of the civil servant with special status - police officer within the authorities provided for in para. (1), with his written consent, every six months, but no later than 31 December 2027.

(13) In the event that, in order to obtain an adequate level of qualified personnel, it is necessary to establish new positions which, according to the job description, contribute to the fulfilment of duties in the field of cybersecurity, AACR and other authorities with competences at sectoral level, as appropriate, may program in the income and expenditure budget for 2025 the increase in salary expenses as a result of the increase in the number of personnel compared to that achieved in 2024, in accordance with the legal provisions in force.

Article 68

Annexes no. 1 "Sectors of high critical importance" and no. 2 "Other sectors of critical importance" are an integral part of this law.

This emergency ordinance transposes the 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) (Text with EEA relevance), published in the Official Journal of the European Union (OJEU) no. L333/80 of 27 December 2022.

PRIME-MINISTER

ION-MARCEL CIOLACU

Bucharest, 30 December 2024.

No. 155.

Annex 1 Sectors of high critical importance

Sector	Sub-sector	Entity type
1. Energy	(a) Electricity	Electricity undertakings defined as "economic operators" in art. 3 point 73 of the Law on Electricity and Natural Gas no. 123/2012 that perform the function of "electricity supply", as defined in art. 3 point 46 of the Electricity and Natural Gas Law no. 123/2012, with subsequent amendments and completions
		Distribution operators, as defined in art. 3 point 70 of Law no. 123/2012
		Transmission system operators, as defined in art. 3 point 71 of Law no. 123/2012
		Producers, as defined as "electricity producers" in art. 3 point 92 of Law no. 123/2012
		The designated operators of the electricity market, as defined in art. 3 point 68 of Law no. 123/2012 Market participants, as defined in art. 3 point 79 of Law no. 123/2012, which provide services of aggregation, demand response or energy storage, as defined in art. 3 points 6, 29, and 121 respectively Operators of a recharging point, as defined in art. 3 point 96 of Law no. 123/2012, which are responsible for the management and operation of a recharging point providing a recharging service to final customers, as defined in art. 3 point 20, including in the name and on behalf of a mobility service provider, as defined in art. 2 point 36 of Regulation (EU) 2023/1804 of the European Parliament and of the Council of 13 September 2023 on the deployment of alternative fuels infrastructure and repealing to Directive 2014/94/EU Economic operators, concessionaires and developer of the offshore wind power plant provided for by Law no. 121/2024 on offshore wind energy
	(b) District heating and district cooling	Operators of district heating or cooling operators, as defined in art. 2 letter t) of Law no. 220/2008 (republished) for establishing the system for promoting the production of energy from renewable energy sources, with subsequent amendments and completions
	(c) Oil	Operators of oil transmission pipeline, as defined as "carriers" in art. 2 point 42 of Petroleum Law no. 238/2004, as subsequently amended and supplemented
		Operators of oil production, refining and processing, storage and transport facilities
		Central storage entities, as defined in art. 2 letters m) and n) of Law no. 85/2018 on the constitution and maintenance of minimum reserves of crude oil and/or petroleum products
	(d) Gas	Supply undertakings, as defined as "suppliers" in art. 100 point 44 of Law no. 123/2012
		Distribution operators, as defined in art. 100 point 63 of Law no. 123/2012
		Transmission and system operators, as defined in art. 100 point 65 of Law no. 123/2012
		Storage operators, as defined in art. 100 point 64 of Law no. 123/2012
		LNG system operators, as defined as "LNG terminal operators" in art. 100 point 60 of Law no. 123/2012

Sector	Sub-sector	Entity type
		Enterprises in the natural gas sector, as defined as "economic operators in the natural gas sector" in art. 100 point 67 of Law no. 123/2012
		Operators of natural gas refining and treatment facilities
	(e) Hydrogen	Hydrogen production, storage and transport operators
	(f) The beneficiaries of the projects financed from non-reimbursable funds, and the type of entity that will have the following content	The beneficiaries provided for by the Government Emergency Ordinance no. 60/2022 on establishing the institutional and financial framework for the implementation and management of the funds allocated to Romania through the Modernisation Fund, as well as for the amendment and completion of certain normative acts, with subsequent amendments and completions
2. Transport	(a) Air transport	Air carriers, as defined in art. 3 point 51 of the Air Code of 18 March 2020, as subsequently amended and supplemented, used for commercial purposes
		Airport managing bodies as defined as “aerodrome managers” in art. 3 point 6 of the Air Code of 18 March 2020, as amended and supplemented, airports as defined in art. 3 point 13, including major airports listed in Section 2 of Annex II to Regulation (EU) no. 1315/2013 of the European Parliament and of the Council of 11 December 2013 on the Union guidelines for the development of the trans-European transport network and repealing Decision no. 661/2010/EU, as well as entities operating auxiliary facilities at airports
		Traffic management control operators providing air traffic control (ATC) services, as defined in art. 2 point 1 of Regulation (EC) no. Regulation (EC) no. 549/2004 of the European Parliament and of the Council of 10 March 2004 establishing the framework for the creation of the Single European Sky (Framework Regulation)
		Aircraft maintenance operators
		Civil aeronautical agents, as defined as "aeronautical agents" in art. 3 point 15 of the Air Code of March 18, 2020, as subsequently amended and supplemented The organisations referred to in art. 2 para. (1) of Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down detailed rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council as regards the requirements relating to the management of information security risks with a potential impact on aviation security imposed on organisations covered by Regulations (EU) no. 748/2012 and (EU) no. 139/2014 of the Commission and amending Regulations (EU) no. 748/2012 and (EU) no. Commission Regulation (EC) No 139/2014 The organisations referred to in art. 2 para. (1) of Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down detailed rules for the application of Regulation (EU) 2018/1139 of the

Sector	Sub-sector	Entity type
		European Parliament and of the Council as regards the requirements relating to the management of information security risks with a potential impact on aviation security, imposed on organisations covered by Regulations (EU) no. 1321/2014, (EU) no. 965/2012, (EU) no. 1178/2011, (EU) 2015/340 and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, as well as the competent authorities covered by Regulations (EU) no. 748/2012, (EU) no. 1321/2014, (EU) no. 965/2012, (EU) no. 1178/2011, (EU) 2015/340 and (EU) no. 139/2014 and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and amending Regulations (EU) no. 1178/2011, (EU) no. 748/2012, (EU) no. 965/2012, (EU) no. 139/2014, (EU) no. Commission Regulation (EU) No 1321/2014, (EU) 2015/340 and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664
	(b) Rail transport	Infrastructure administrators, as defined in art. 3 point 3 of Law no. 202/2016
		Railway undertakings, as defined as "railway transport operators" in art. 3 point 18 of Law no. 202/2016, including operators of a service infrastructure, as defined in art. 3 point 19
	(c) Water transport	Inland, sea and coastal water freight and passenger transport companies, as defined for maritime transport in Annex I to Regulation (EC) no. Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on strengthening the security of ships and port facilities, not including individual ships operated by those companies
		Managing bodies of ports, as defined in art. 3 of the Order of the Minister of Transport no. 290/2007 for the introduction of measures to strengthen port security, including their port facilities, as defined in art. 2 point 11 of Regulation (EC) no. 725/2004, and the entities that carry out works and operate equipment within ports
		Maritime traffic service operators (STM), as defined in art. 3 letter t) of Government Decision no. 1016/2010 for the establishment of the Information and Monitoring System for the traffic of maritime vessels entering/leaving the national navigable waters of Romania, with subsequent amendments and completions
	(d) Road transport	Road authorities as defined in point 12 of art. 2 of Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is only a non-essential part of their general activity
		Operators of intelligent transport systems, as defined in art. 4 letter a) of Government Ordinance no. 7/2012 on the implementation of intelligent transport systems in the field of road transport and for the creation of interfaces with other modes of transport, approved by Law no. 221/2012
3. Banking sector		Credit institutions, as defined in art. 4 point 1 of Regulation (EU) no. 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) no. 648/2012

Sector	Sub-sector	Entity type
4. Financial market infrastructures		Operators of trading venues, as defined in art. 3 para. (1) point 40 of Law no. 126/2018 on markets in financial instruments, as subsequently amended and supplemented
		Central counterparties (CCPs), as defined in art. 3 para. (1) point 16 of Law no. 126/2018
5. Health sector		Healthcare providers, as defined by art. 347 letter c) of Law no. 95/2006 (republished) on the health reform, with subsequent amendments and completions
		EU reference laboratories as defined in art. 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision no. 1082/2013/EU
		Entities carrying out research and development of medicinal products Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in Section C, Division 21 of NACE Rev. 2 Entities manufacturing medical devices considered to be essential in the context of a public health emergency (list of essential devices for public health emergency) within the meaning of art. 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on strengthening the role of the European Medicines Agency in crisis preparedness in the field of medicines and medical devices, and managing them
6. Drinking water		Water suppliers and distributors, as defined as "water suppliers" in art. 2 letter c) of Government Ordinance no. 7/2023 on the quality of water intended for human consumption, as subsequently amended and supplemented, intended for human consumption, as defined in art. 2 letter a) of the same ordinance, except for the water used in any food-type unit for the production, processing, preservation or marketing of products or substances intended for human consumption and excluding distributors for whom the distribution of water intended for human consumption represents a non-essential part of the their general activity of distributing other commodities and goods that are not considered essential services
7. Wastewater		Undertakings that collect, dispose of or treat urban wastewater, domestic wastewater or industrial wastewater, as defined in art. 2 points 1-3 of Annex no. 1 - Technical Norms of 28 February 2002 on the collection, treatment and discharge of urban wastewater, NTPA-011 to Government Decision no. 188/2002 for the approval of rules on the conditions of discharge of wastewater into the aquatic environment, excluding enterprises for which the collection, disposal or treatment of urban wastewater, domestic wastewater or industrial wastewater is a non-essential part of their general activity, as subsequently amended and supplemented
8. Digital infrastructure		IXP (internet exchange point) providers
		DNS service providers, except root name server operators
		TLD Name Registries

Sector	Sub-sector	Entity type
		Cloud computing service providers
		Data centre service providers
		Content Delivery Network Providers
		Trusted service providers
		Providers of public electronic communications networks
		Providers of publicly available electronic communications services
9. ICT service management (business-to-business)		Managed Service Providers Managed Security Service Providers
10. Public administration		Central public administration entities, except for institutions in the field of defence, public order and national security, the National Registry Office for Classified Information, higher education institutions, the legal field, justice, including the Public Ministry, the Romanian Parliament, the General Secretariat of the Government, the Prime Minister's Chancellery, the Presidential Administration, ASF, BNR and ANCOM.
11. Space		Operators of terrestrial infrastructure owned, managed and operated by the Romanian state or by private entities on the territory of Romania, which support the provision of space services, excluding providers of public electronic communications networks.

Annex 2 Other sectors of critical importance

Sector	Subsector	Entity type
1. Postal and courier services		Postal service providers, as defined in art. 2 point 2 of the Government Emergency Ordinance no. 13/2013 on postal services, as subsequently amended and supplemented, by Law no. 187/2013, including courier service providers
2. Waste management		Undertakings carrying out waste management, as defined in point 19 of Annex no. 1 to the Government Emergency Ordinance no. 92/2021 on the waste regime, approved with amendments and completions by Law no. 17/2023, except for undertakings for which waste management is not the main economic activity
3. Manufacturing, production and distribution of chemicals		Undertakings producing substances and distributing substances or mixtures, as referred to in art. 3 points 9 and 14 of Regulation (EC) no. 1907/2006 of the European Parliament and of the Council of 18 December 2006 on the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing the European Chemicals Agency, amending Directive 1999/45/EC and repealing Regulation (EEC) no. 793/93 of the Council and of Regulation (EC) no. 1488/94, as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC and undertakings producing articles, as defined in art. 3 point 3 of that Regulation, from substances or mixtures

Sector	Subsector	Entity type
4. Production, processing and distribution of food		Food businesses as defined in art. 3 point 2 of Regulation (EC) no. Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in the field of food safety, which are involved in wholesale distribution and industrial production and processing
5. Manufacturing	(a) Manufacture of medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices, as defined in art. 2 point 1 of Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) no. 178/2002 and Regulation (EC) no. 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, and entities manufacturing in vitro diagnostic medical devices as defined in point 2 of art. 2 of Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, with the exception of entities manufacturing medical devices listed in point 5 of Annex I
	(b) Manufacture of computers, electronic and optical products	Undertakings carrying out any of the economic activities mentioned in NACE Revision 26
	(c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities mentioned in division 27 of NACE Rev. 3, according to the Order of the President of the National Institute of Statistics
	d) Manufacture of other machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities mentioned in division 28 of NACE Rev. 3, according to the Order of the President of the National Institute of Statistics
	(e) Manufacture of motor vehicles, trailers and semi-trailers	Undertakings carrying out any of the economic activities mentioned in division 29 of NACE Rev. 3, according to the Order of the President of the National Institute of Statistics
	(f) Manufacture of other transport equipment	Undertakings carrying out any of the economic activities mentioned in NACE Rev. 30 division, according to the Order of the President of the National Institute of Statistics
6. Digital Providers		Providers of online marketplaces
		Providers of online search engine
		Providers of social networking service platforms
7. Research		Research organisations