National Cybersecurity System Act

Filip Radoniewicz

Abstract The Act of the 5th of July 2018 on the National Cybersecurity System (hereinafter referred to as “NCSA”), as indicated in the explanatory memorandum to this act, is on the one hand an attempt to comprehensively regulate the national cybersecurity system, which is a response to the constantly growing and dynamically changing cyber threats, which may affect the security of the state, the economy and society, and on the other hand it is the implementation of the Directive (EU) 2016/1148 of the European Parliament and of the Council of the 6th of July 2016 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive). The purpose of this chapter is a brief description of the act and a synthetic presentation of the solutions it contains, which will be discussed in detail later in the monograph.

1 Introduction

The Act of the 5th of July 2018 on the National Cybersecurity System¹ (hereinafter the NCSA), as indicated in the substantiation to its draft version is, on the one hand, an attempt at comprehensively regulating the national cybersecurity system, in response to the ever-growing and dynamically evolving cyber threats, which may potentially compromise the security of the State, the economy and society; on the other hand, it is intended to implement the above-mentioned NIS Directive.

The national cybersecurity system is organised to ensure cybersecurity at the national level, including the undisrupted provision of essential services and digital services, by attaining a sufficient level of security of information systems serving the

¹ Act of 5 July 2018 on the National Cybersecurity System, consolidated text Polish Journal of Laws of 2020 item 1369 as amended.

F. Radoniewicz (✉)

Akademickie Centrum Polityki Cyberbezpieczeństwa/Academic Center for Cybersecurity Policy, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland

e-mail: filip.radoniewicz@radoniewicz.eu

purpose of providing such services, and by ensuring incident handling (Article 3 of the NCSA).

The Act regulates three problem areas: the organisation of the national cybersecurity system, and the duties and obligations of the entities, which form its part; the procedure for supervising and inspecting compliance with the provisions of the Act; and the scope of the Cybersecurity Strategy of the Republic of Poland (which is discussed in Chapter 13 of the NCSA).

The legislator has envisaged some exclusions in this respect, whether in whole or in part. Namely, providers of trust services and entities conducting treatment activities, established by the Head of the Internal Security Agency or the Head of the Intelligence service are wholly excluded from the Act, while telecommunications enterprises are excluded in the part regarding security and incident reporting requirements.

For the purpose of the NCSA, 19 definitions were formulated which, in view of the significance of this regulation, should be considered systemic definitions. First and foremost, the information system is understood as the ICT system (the teleinformation system) referred to in Article 3(3) of the Act of the 17th of February 2005 on the Computerisation of the Operations of Entities Performing Public Tasks, along with electronic data processed in that system (Article 2(14) of the NCSA). Second, cybersecurity is viewed as the ability of information systems to resist any action that compromises the confidentiality, integrity, availability and authenticity of processed data or related services rendered via such systems (Article 2(4) of the NCSA).²

In Article 2(5) of the NCSA, an incident is defined as an event, which has, or may have, an adverse impact on cybersecurity. The legislator has distinguished four categories of incidents: a critical incident (Article 2 (6) of the NCSA), a serious incident (Article 2 (7) of the NCSA), a substantial incident (Article 2 (8) of the NCSA), and an incident occurring within a public entity (Article 2 (9) of the NCSA):

1. serious incidents (Article 2 (7) of the NCSA), which cause, or may cause, serious detriment to quality or which result, or may result, in the discontinuation of the provision of an essential service (as defined in Article 14 (3) of the NIS Directive, incidents having a significant impact on the continuity of essential services);
2. substantial incidents (Article 2 (8) of the NCSA), which have a substantial impact on the provision of a digital service within the meaning of Article 4 of the Implementing Regulation 2017/151 (as defined in Article 16 (3) of the NIS Directive, incidents having a substantial impact on the provision of digital services);
3. incidents occurring within a public entity (Article 2 (9) of the NCSA), the classification of an incident to this category is not based on its significance (the impact threshold) but on the object of such impact, which is the ICT network used for the processing of data connected with the implementation of public duties, by public entities referred to in Article 4(7)-(15) of the NCSA, hence, all incidents, which cause, or may cause, serious detriment or discontinuation of a public duty;

²See more e.g. Radoniewicz (2019), pp. 27–51.

4. critical incidents (Article 2 (6) of the NCSA), which are incidents of the most serious character, resulting in serious detriment to security or public order, international interests, economic interests, activities of public institutions, civic rights and freedoms, or human life and health, classified by the relevant CSIRT MON, CSIRT NASK or CSIRT GOV.³

2 Entities of the National Cybersecurity System

The national cybersecurity system covers, in particular, operators of essential services (e.g. banks and enterprises from the energy sector), providers of digital services (e.g. entrepreneurs conducting activities via e-commerce platforms), authorities competent for cybersecurity, i.e. public institutions whose competences include supervising a given essential sector of economy (competent ministers, i.e. the minister competent for energy, the minister competent for transport, the minister competent for of maritime economy, the minister competent for inland navigation, the minister competent for health, the Minister of National Defence, the minister—competent for computerisation and the Polish Financial Supervision Authority), the Computer Security Incident Response Teams established within the Internal Security Agency (CSIRT GOV), the Research and Academic Computer Network, National Research Institute (CSIRT NASK), the Ministry of National Defence (CSIRT MON), sectoral cybersecurity teams, the Point of Single Contact for cybersecurity, the Government Plenipotentiary for Cybersecurity, the College for Cybersecurity, and public entities listed in Article 4 of the NCSA. The above-listed entities can be divided into:

1. administration entities—mainly serving supervisory and inspection functions (listed in Article 4 (17)-(20) of the NCSA) or coordinating incident handling (listed in Article 4 (3)-(6) of the NCSA);
2. participants: operators of essential services, digital service providers, and public entities listed in Chapter 5 of the NCSA;
3. other entities, entities difficult to unambiguously classify, e.g. providers of cybersecurity services.⁴

3 CSIRT MON, CSIRT NASK and CSIRT GOV

While implementing the provisions of the NIS Directive on establishing Computer Security Incident Response Teams (CSIRTs), new entities were not established, but the use was made of those already operating at the national level, on which the

³See more Chałubińska-Jentkiewicz et al. (2021), *passim*.

⁴Radoniewicz (2019), p. 54.

obligations arising from the Directive were imposed. These included: CERT.GOV.PL, MIL-CERT.PL and CERT POLSKA, i.e. currently CSIRT GOV, CSIRT MIL and CSIRT NASK, respectively.

CSIRT GOV, the Government Computer Security Incident Response Team, operating since January 2008 within the Internal Security Agency (as CERT.GOV.PL). It is in charge of coordinating the handling of incidents reported by the entities listed in Article 26 (7) of the NCSA (government administration, the National Bank of Poland, and Bank Gospodarstwa Krajowego). In addition, it is entrusted with identifying, preventing and detecting threats to security, which are important for ensuring the continuity of the functioning of the national ICT systems, utilised by public administration authorities or a system of ICT networks forming part of critical infrastructure. CSIRT MON (formerly MIL-CERT.PL), operating within the Computer Incident Response System of the Ministry of National Defence (SRnIK RON), performs duties in the field of coordinating the processes of preventing, detecting and responding to computer incidents in the ICT systems and networks of that Ministry. CSIRT MON coordinates the process of handling incidents reported by the entities subordinated to or supervised by the Ministry of National Defence, including entities whose ICT systems or networks are included in a consolidated register of facilities, installations, devices and services forming parts of critical infrastructure, referred to in Article 5b (7) (1) of the Act of the 26th of April 2007 on Crisis Management, and entrepreneurs of particular economic and defensive significance. NASK (the Research and Academic Computer Network) is a national research institute operating since 1993, which conducts scientific activities, runs the national (.pl) domains register, and provides advanced ICT services. Since 1996, CERT POLAND, currently CSIRT NASK, has been operating within its framework, coordinating the process of handling incidents, which violate network security in the “civil area” and, which occur within public networks, i.e. incidents reported by other entities (not classified to any of the above-mentioned groups), including by operators of essential services (excluding operators of critical infrastructure), digital services providers, and local government authorities. Generally speaking, CSIRT NASK’s competences cover all incidents reported by those entities, which do not fall within the competences of CSIRT GOV and CSIRT MON (while the latter two are always, regardless of the category of the reporting entity, in charge of terrorist incidents, and CSIRT MON is also in charge of any incidents related to national defence). It is thus referred to as the CERT of last resort, being the entity to whom all citizens (or, more generally, all natural persons and organisational units) may report incidents. Furthermore, if an entity cannot establish direct contact or receive the expected support from the party directly involved in the incident, the reporting party files its query with the CSIRT as a last resort.⁵ The tasks of, CSIRT MON, CSIRT NASK and CSIRT GOV are detailed described the chapter entitled “The main tasks of the team network to respond to computer security incidents in the light of the Act on the national cybersecurity system in Poland”.

⁵See Banasiński and Nowak (2018), pp. 161–162; Trąbiński (2018), pp. 76–78.

4 The Competent Authorities for Cybersecurity

The competent authorities for cybersecurity are supreme authorities (i.e. competent ministers, depending on the sector indicated in Appendix I to the Act, in which a given operator of an essential service or a digital service provider conducts its activities, the minister competent for energy, the minister competent for transport, the minister competent for maritime economy, the minister competent for inland navigation, the minister competent for health, the Minister of National Defence, or the minister competent for computerisation), and one central authority (the Polish Financial Supervision Authority), issuing decisions on recognising an entity as the operator of an essential service (and also confirming the expiry of decisions made to that effect) and supervising those entities. Their duties are discussed in the chapter “The authorities competent for cybersecurity”.

5 The Minister Competent for Computerisation and the Minister of National Defense

The minister competent for computerisation and the Minister of National Defense play a special role in the national cybersecurity system. The cited regulations referred to them are described in detail in separate chapters in part II of the monograph. The contact point run by the minister competent for computerisation ensures the exchange of information between various entities responsible for cybersecurity. Its duties include collecting serious or substantial incident reports from other EU Member States, and passing them to CSIRT MON, CSIRT NASK, CSIRT GOV or sectoral cybersecurity teams; passing serious or substantial incident reports concerning two or more EU Member States to other Member States; representing the Republic of Poland in the Cooperation Group; cooperating with the European Commission in the field of cybersecurity; coordinating the cooperation between authorities competent for cybersecurity and public authorities with the competent authorities in EU Member States; and ensuring information exchange for the Cooperation Group and CSIRT network purposes.⁶

⁶See more: chapter 16 “Role of Minister competent for computerisation in Cybersecurity system”.

6 The Government Plenipotentiary for Cybersecurity

This is a single-person function appointed and recalled by the President of the Council of Ministers to coordinate activities and to implement the government's policy directed at ensuring cybersecurity. The Plenipotentiary's primary duties include:

- (1) analysing and assessing the functioning of the national cybersecurity system based;
- (2) supervising the risk management process within the national cybersecurity system based;
- (3) reviewing governmental documents, including draft legal acts, pertinent to the implementation of cybersecurity-related duties;
- (4) popularising new solutions and initiating activities to ensure cybersecurity at the national level;
- (5) initiating cybersecurity training at the national level;
- (6) issuing recommendations on the use of IT equipment or software at the CSIRT request (Article 62(1) of the NSC Act).

7 The College for Cybersecurity

The College for Cybersecurity is a collegial opinion-making and advisory authority, operating within the Council of Ministers, regarding cybersecurity issues and activities conducted in this field by CSIRT, the Ministry of National Defence, CSIRT NASK, CSIRT GOV, sectoral cybersecurity teams and authorities competent for cybersecurity. The College is led by the President of the Council of Ministers and is composed of the minister competent for internal affairs, the Minister competent for computerisation, the Minister of National Defence, the minister competent for foreign affairs, the Head of the Chancellery of the President of the Council of Ministers, the Head of the National Security Bureau, and the Minister competent for coordinating the activities of special forces. The College meetings are also attended by the Director of the Government Centre for Security, the Head or Deputy Head of the Internal Security Agency, the Head or Deputy Head of the Military Counterintelligence Service, and the Director of the Research and Academic Computer Network and the National Research Institute.

In addition, the College draws up recommendations for the Council of Ministers on the activities directed at ensuring cybersecurity at the national level (Article 65 (2) of the NCSA).

8 Incident Response Teams for a Given Sector or Subsector

The Act has envisaged the possibility for a computer security incident response team to be established by the authorities competent in cybersecurity, for any of the sectors or subsectors listed in the appendix to the Act (which is, therefore, not an obligatory body), i.e. a sectoral cybersecurity team (as referred to in Article 4 (6) of the NCSA) in charge of receiving serious incident reports within that sector or subsector. Such a team shall also be responsible for providing support in the handling of such incidents, supporting operators of essential services in performing their duties arising from the Act, analysing serious incidents, identifying associations between incidents, and formulating conclusions on incident handling, as well as for cooperating with the competent CSIRT (Article 44 (1) of the NCSA). Sectoral cybersecurity teams were not included in the initial draft act. A suggestion to include the possibility for these entities to be established was put forward during social consultations, and it appeared in numerous opinions, in which the fact that such teams would take account of the specificity of a given sector, thus enabling the support to be adjusted to operators of essential services, was seen as a major advantage. More about the Government Plenipotentiary and the College for Cybersecurity, see the chapter “The duties and legal status of the Government Plenipotentiary for Cybersecurity and the College for Cybersecurity”.

9 Operators of Essential Services

These are entities whose organisational units are situated in the territory of the Republic of Poland, and in respect of whom the authority competent for cybersecurity has issued a decision on recognising them as operators of essential services (i.e. services of the highest significance for the maintenance of social or economic activities, included in the list of essential services), e.g. banks, enterprises from the energy sector, etc. It seems that a situation cannot be ruled out in which natural persons conducting business activities are classified as such, along with legal persons and organisational units without a legal personality whose legal capacity arises from separate provisions (e.g. commercial law companies and partnerships).

The authorities competent for cybersecurity issue a decision on recognising an entity as the operator of an essential service. The list of operators of essential services is maintained by the minister competent for computerisation. Operators of essential services are obligated, in particular, to ensure the security of the information systems they use for the provision of essential services. Operators of essential services cooperate with the sectoral cybersecurity team (if applicable). In addition, they are obliged to ensure the carrying out, at least on a biennial basis, the security audit of the information system used for the provision of the essential service.

With the purpose of performing their cybersecurity duties, operators of essential services establish internal structures responsible for cybersecurity or enter into

agreements with third parties for the provision of cybersecurity services. The organisational and technical conditions for entities providing cybersecurity services, and internal structures responsible for cybersecurity, are determined by the minister competent for computerisation, by way of a regulation, which must consider the Polish Norms, along with the need to ensure the security of the internal structures responsible for cybersecurity, entities providing cybersecurity services to operators of essential services, and information processed within such structures or entities.

10 Digital Service Providers

Digital service providers are legal persons or organisational units without a legal personality with a registered office or management bodies in the Republic of Poland, or whose representatives operate organisational units in the territory of the Republic of Poland, and which provide digital services, i.e. services rendered electronically, within the meaning of the Act of the 18th of July 2002 on the Provision of Services Electronically (see more in the latter part of this article), as listed in Appendix 2 to the Act, i.e. e-commerce platforms, cloud computing services and search engines (Article 17 of the NCSA). Digital service providers take the appropriate and commensurate technical and organisational measures, as defined in Implementing Regulation 2018/151, to manage the risks posed to information systems used for the provision of digital services. These measures must guarantee cybersecurity commensurate with the actual risk. The obligations of operators of essential services and digital service providers and the liability of these entities are discussed in Part III of this monograph.

11 Entities Providing Cybersecurity Services

Entities providing cybersecurity services are entities, with which operators of essential services may conclude agreements with the purpose of performing their cybersecurity duties (the outsourcing of security services). These involve estimating the risk to essential services and managing that risk; implementing the appropriate technical and organisational measures, commensurate with the estimated risk; collecting information on threats and vulnerabilities; incident management; using preventive measures to limit the incident's impact on the security of the information system; using the means of communications enabling the proper and safe communication within the national cybersecurity system (Article 8); appointing a person in charge of contacts with authorities competent for cybersecurity, the competent CSIRT and the Point of Single Contact supervised by the minister competent for computerisation, and (if applicable) the sectoral cybersecurity team, and notifying these bodies of this fact; conducting educational activities addressed to users; providing the competent authority with information specifying in which EU Member

States these entities have been recognised as operators of essential services, and the date of termination of the provision of such services (Article 9 of the NCSA); developing, implementing and updating the required documentation (Article 10 (1)-(3) of the NCSA); handling incidents within their own systems; reporting serious incidents; cooperating in the handling of serious and critical incidents with the competent CSIRT, and (if applicable) the sectoral cybersecurity team; eliminating the identified vulnerabilities (Article 11(1)-(3) and Article 12 of the NCSA); and passing to the competent CSIRT information on other incidents, threats to cybersecurity pertinent to risk estimation, vulnerabilities and technologies used (Article 13 of the NCSA).

12 Entities Referred to in Article 4(7)-(15) of the Act on the National Cybersecurity System

Another group of entities included in the national cybersecurity system is indicated in Article 4(7) of the NCSA. These are, in the first place public finance sector units referred to in Article 9 (1)-(6),(8),(9),(11) and (12) of the Act of the 27th of August 2009 on Public Finance.⁷

The concept of the finance sector, rather than being expressly defined, has been described by reference to entities forming its part. Although the express legal definition is missing, major characteristic features of the finance sector entities may be outlined.⁸

More specifically, the finance sector is composed of organisational units set up under the applicable acts (the PF Act and specific acts) with the sole purpose of fulfilling public duties, which are financed from public resources and are subject to planning, balancing, control, accountancy and reporting, as well as discipline based on uniform principles. Some of the entities forming part of the public finance sector are listed by their names (the National Health Fund, the Social Insurance Institution, the Agricultural Social Insurance Fund, and the Polish Academy of Sciences) while others by their type (budgetary units, public authorities, State-owned or local government owned legal persons).⁹

The entities indicated (indirectly) in Article 4 (7) of the NCSA, i.e. public finance sector entities referred to in Article 9 (1)-(6), (8), (9), (11) and (12) of the PF Act, include:

- (1) public authorities, including government administration bodies, State inspection and law enforcement bodies, as well as courts and tribunals,

⁷ Act of 27 August 2009 on Public Finance consolidated text, Polish Journal of Laws of 2019, item 869, as amended (hereinafter: the PFA).

⁸ Cilak (2020).

⁹ Lipiec-Warzecha (2011), p. 84.

- (2) local government bodies and their unions,
- (3) budgetary units,
- (4) local government-owned budgetary establishments,
- (5) executive agencies,
- (6) budget management institutions,
- (7) the Social Insurance Institution and the resources it manages, as well as the Agricultural Social Insurance Fund and the resources managed by the President of the Agricultural Social Insurance Fund,
- (8) the National Health Fund (in Polish: NFZ),
- (9) state-owned higher education institutions, and
- (10) The Polish Academy of Sciences and the organisational units it establishes.

Other entities, not previously discussed, listed in Article 4(7)-(15) of the NCSA:

- (1) research institutes;
- (2) the National Bank of Poland;
- (3) Bank Gospodarstwa Krajowego;
- (4) the Office of Technical Inspection;
- (5) the Polish Air Navigation Services Agency;
- (6) the Polish Centre for Accreditation;
- (7) the National Fund for Environmental Protection and Water Management, and regional funds for environmental protection and water management;
- (8) commercial law companies and partnerships performing public utility duties within the meaning of Article 1(2) of the Act of the 20th of December 1996 on Municipal Services.¹⁰

The regulations referred to public entities indicated in Article 4 (7)-(15) of the NCSA are described in the chapter “Obligations of public entities in the National Cybersecurity system” in III part of the monograph.

The compliance with the provisions of the NCSA is controlled and supervised¹¹ by:

1. the minister competent for computerisation, as regards the compliance of the entities providing cybersecurity services with statutory requirements;
2. authorities competent for Cybersecurity, as regards:
 - (a) the performance of the statutory obligations to counteract cybersecurity threats and to report serious incidents by operators of essential services,
 - (b) the compliance of digital service providers with security requirements as part of the digital services rendered by those entities, as defined in Implementing

¹⁰Act of 20 December 1996 on Municipal Services, consolidated text, Polish Journal of Laws of 2019, item 712, as amended.

¹¹This matter is dedicated the chapter 20 “The system of control and supervision of operators of essential services, digital-service providers and entities providing cybersecurity services” in part III of the book.

Regulation 2018/151, the performance of their statutory obligations to report substantial incidents.

13 Penalties Provided for in the Act on the National Security System

Article 21 of the NIS Directive puts Member States under the obligation to envisage effective, proportionate and dissuasive penalties for the infringements of national provisions adopted pursuant to this Directive, and to take all measures necessary to ensure that they are implemented.

The Polish legislator has laid down regulation providing for administrative liability to be incurred by three groups of entities:

1. operators of essential services,
2. digital service providers, and
3. managers of operators of essential services.

In respect of operators of essential services and digital service providers, the legislator has only envisaged financial penalties, their amounts ranging from 1.00 PLN (where no lower limit of the penalty has been set) to 200,000 PLN. However, if the authority competent for cybersecurity, having conducted an inspection, finds that a given operator of an essential service or a given digital service provider violates the provisions of that Act, causing:

1. a direct and serious threat to cybersecurity in the field of defence, State security, security and public order, or human life and health,
2. a threat of causing a serious property damage or serious disruptions in the provision of essential services,

the authority competent for cybersecurity imposes a monetary penalty of up to 1,000,000 PLN (Article 73 (5) of the NSC Act).

Almost all violations for which penalties have been envisaged in the national cybersecurity system refer to the non-performance or improper performance by the operator of an essential service of the obligation imposed by the provisions of the Act (failure to report a serious incident to the responsible CSIRT MON, CSIRT NASK or CSIRT GOV within twenty four hours of its detection; therefore, an incident reported after the expiry of the said period will also be construed as a violation). Two other violations refer to hindering the inspection process and a failure to conform to post-inspection recommendations.

The proceedings regarding financial penalties imposed under the NCSA are governed by the provisions of the Code of Administrative Procedure,¹² which arises from the content of Article 189a of the CAP requiring the application of the

¹²Act of 14 June 1960—the Code of Administrative Procedure (consolidated text, Polish Journal of Laws of 2020, item 256, as amended (hereinafter: “CAP”).

provisions of Section IVa of the CAP in respect of imposing or applying an administrative financial penalty or granting a relief from the enforcement of the penalty.¹³

14 The Cybersecurity Strategy

The Cybersecurity Strategy of the Republic of Poland is a document adopted by way of a resolution of the Council of Ministers, determining the strategic objectives, and the relevant political and regulatory measures directed at attaining and maintaining a high level of cybersecurity. It is developed for a five-year period with possible amendments throughout its duration (Article 68 and Article 69 (1) of the NCSA).¹⁴ The draft Strategy is developed by the minister in charge of computerisation in cooperation with the Plenipotentiary, other ministers, and the responsible managers of central offices. The work on the draft version of the Strategy may also be attended by a representative of the President of the Republic of Poland.

The Strategy specifies, in particular:

- (1) the objectives and priorities regarding cybersecurity;
- (2) the entities engaged in the implementation of the Strategy;
- (3) the measures directed at implementing the objectives assumed in the Strategy;
- (4) the means for readiness, response and restoration, including principles of public-private cooperation;
- (5) an approach to risk assessment;
- (6) activities related to educational, informational and training programmes in the field of cybersecurity;
- (7) activities related to research and development plans in the field of cybersecurity.

Strategy is dedicated the separate chapter in this part of the monograph.

15 Legal Acts Modified by the Act on the National Cybersecurity System

The Act on the National Cybersecurity System adjusts a number of legal acts to the provisions of the NIS Directive:

¹³More about monetary penalties—see chapter 21 “Monetary penalties in the National Cybersecurity System Act” in part III of this book.

¹⁴The currently binding strategy was adopted by way of Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024 (Official Gazette of the Government of the Republic of Poland of 2019, item 1037).

- (1) the Act of the 7th of September 1991 on the Education System;¹⁵
- (2) the Act of the 4th of September 1997 on Branches of Government Administration;¹⁶
- (3) the Act of the 24th of May 2002 on the Internal Security Agency and on the Intelligence Service;¹⁷
- (4) the Act of the 29th of January 2004—Public Procurement Law;¹⁸
- (5) the Act of the 16th of July 2004—Telecommunications Law;¹⁹
- (6) the Act of 26 April 2007 on Crisis Management;²⁰

Furthermore, in connection with the amendment to Article 5a (2) of the Act on Crisis Management introduced under the reference Act (see Article 82 of the NCSA), it was deemed necessary to amend the Agreement of the 19th of August 2010 on determining the detailed scope and means of cooperation of the Government Centre for Security and the Internal Security Agency.²¹

16 Legal Acts Issued Under the Authorisations Included in the Act on the National Cybersecurity System

Under the authorisations stipulated in the NCSA, seven implementing acts have been issued to date.²²

1. The Regulation of the Council of Ministers of the 31st of October 2018 on serious incidents thresholds;²³

¹⁵Act of 7 September 1991 on the Education System, consolidated text, Journal of Laws of 2020, item 13277, as amended.

¹⁶Act of 4 September 1997 on Branches of Government Administration, consolidated text, Polish Journal of Laws of 2020, item 1220, as amended.

¹⁷Act of 24 May 2002 on the Internal Security Agency and on the Intelligence Service, consolidated text, Polish Journal of Laws of 2020, item 27, as amended.

¹⁸Act of 29 January 2004—Public Procurement Law, consolidated text, Polish Journal of Laws of 2019, item 1843, as amended.

¹⁹Act of 16 July 2004—Telecommunications Law, consolidated text, Polish Journal of Laws of 2019, item 2460, as amended.

²⁰Act of 26 April 2007 on Crisis Management, consolidated text, Polish Journal of Laws of 2020, item 1856, as amended.

²¹Official Journal of the ISA of 2010 No. 3, item 28, as amended.

²²I.e. by 1 December 2020.

²³The Regulation of the Council of Ministers of 31 October 2018 on serious incidents thresholds Polish Journal of Laws of 2018, item 2180.

2. The Regulation of the Council of Ministers of the 16th of October 2018 on documents regarding cybersecurity of the information system used for the provision of essential services;²⁴
3. The Regulation of the Council of Ministers of the 2nd of October 2018 on the scope of activities and the working procedure of the College for Cybersecurity;²⁵
4. The Regulation of the Council of Ministers of the 11th of September 2018 on a list of essential services and significance thresholds of the consequences of incidents disrupting the provision of essential services;²⁶
5. The Regulation of the Minister of Digital Affairs of the 10th of September 2018 on the organisational and technical conditions for entities providing cybersecurity services, and internal structures responsible for cybersecurity;²⁷
6. The Regulation of the Minister of Digital Affairs of the 12th of October 2018 on the list of certificates authorising the performance of audits;²⁸
7. The Regulation of the Minister of Digital Affairs of the 4th of December 2019 on the organisational and technical conditions for entities providing cybersecurity services, and internal organisational structures of operators of essential services responsible for cybersecurity;²⁹

Under Article 42 (1) (5), in connection with Article 41(3) and (7) of the NCSA, Ordinance No. 20 of the Minister of Maritime Economy and Inland Navigation of the 16th of April 2019 on the guidelines regarding the reporting of incidents within the national cybersecurity system in the water transport subsector, and in the potable water supply and distribution sector,³⁰ was issued.

In addition, under Article 52 (1) of the Act of the 6th of September 2001 on Road Transport,³¹ in connection with Article 21 (1) of the NCSA, Ordinance No. 43/2018

²⁴The Regulation of the Council of Ministers of 16 October 2018 on documents regarding cybersecurity of the information system used for the provision of essential services ,Polish Journal of Laws of 2018, item 2080.

²⁵The Regulation of the Council of Ministers of 2 October 2018 on the scope of activities and the working procedure of the Committee for Cybersecurity Polish Journal of Laws of 2018, item 1952.

²⁶The Regulation of the Council of Ministers of 11 September 2018 on a list of essential services and significance thresholds of the consequences of incidents disrupting the provision of essential services Polish Journal of Laws of 2018, item 1806.

²⁷The Regulation of the Minister of Digital Affairs of 10 September 2018 on the organisational and technical conditions for entities providing cybersecurity services, and internal structures responsible for cybersecurity Polish Journal of Laws of 2018, item 1780.

²⁸The Regulation of the Minister of Digital Affairs of 12 October 2018 on the list of certificates authorising the performance of audits Polish Journal of Laws of 2018, item 1999.

²⁹The Regulation of the Minister of Digital Affairs of 4 December 2019 on the organisational and technical conditions for entities providing cybersecurity services, and internal organisational structures of operators of essential services responsible for cybersecurity Polish Journal of Laws of 2019, item 2479.

³⁰Official Journal of the Ministry of Maritime Economy and Inland Navigation of 2019, item 20.

³¹Act of 6 September 2001 on Road Transport Polish Journal of Laws of 2017, item 2200, as amended.

of the Chief Inspector of Road Transport on appointing the Plenipotentiary for cybersecurity at the Chief Inspectorate of Road Transport of the 20th of September 2018 was issued.³²

Under 175a(2)(a) of the Telecommunications Law, added by way of Article 80 of the NCSA, the Minister of Digital Affairs issued the Regulation of the 20th of September 2018 on the criteria of recognising the violation of security or integrity of networks or telecommunications services as a violation significantly affecting the functioning of networks or services.³³ At the same time, under Article 175a (2) of Telecommunications Law, the Minister of Digital Affairs issued a new Regulation of the 20th of September 2018 on the template form for providing information on the violation of security or integrity of networks or telecommunications services as a violation significantly affecting the functioning of networks or services,³⁴ which replaced the previously binding regulation bearing the same title. However, the authorisation granted in Article 32aa(9) of the Act on the Internal Security Agency and the Intelligence Service, added by way of Article 79 of the NCSA, that the President of the Council of Ministers determine, by way of a regulation, the conditions and procedure for conducting, coordinating and implementing the warning system, and in particular to determine the measures necessary for its establishment and maintenance, and the template agreement referred to in Par. 7 (in which the ISA makes arrangements with the critical infrastructure operator regarding the technical aspects of participation in the warning system and the system configuration model), driven by the need to ensure security of the ICT systems significant from the point of view of the continuity of the functioning of the State, has not been implemented yet.

Some other documents were issued under the NCSA, e.g.:

1. The Communication of the Minister of Digital Affairs of the 7th of January 2020 on the agreement between CSIRT GOV and CSIRT NASK regarding the delegation of duties;³⁵
2. Communication No. 1 of the Head of the Internal Security Agency of the 29th of August 2019 regarding the conclusion of an agreement on the delegation of duties related to incidents reported by the Polish Air Navigation Services Agency;³⁶
3. Communication No. 2 of the Head of the Internal Security Agency of the 28th of November 2019 regarding the conclusion of an agreement on the delegation of

³²Official Journal of the Chief Inspector of Road Transport of 2018, item 43.

³³Polish Journal of Laws of 2018, item 1830.

³⁴Polish Journal of Laws of 2018, item 1831.

³⁵Official Journal of the Ministry of Digital Affairs of 2020, item 1.

³⁶Communication No. 1 of the Head of the Internal Security Agency of 29 August 2019 regarding the conclusion of an agreement on the delegation of duties related to incidents reported by the Polish Air Navigation Services Agency Official Journal of the Internal Security Agency of 2019, item 15.

- duties related to incidents reported by the Research and Academic Computer Network to the National Research Institute;³⁷
4. Communication No. 3 of the Head of the Internal Security Agency of the 28th of November 2019 regarding the conclusion of an agreement on the delegation of duties related to incidents reported by companies being members of the Capital Group of PGE Polska Grupa Energetyczna S.A.;³⁸
 5. Resolution No. 125 of the Council of Ministers of the 22nd of October 2019 on the National Policy Frameworks on Cybersecurity of the Republic of Poland for 2019–2024;³⁹
 6. The Communication of the Minister of Digital Affairs of the 19th of September 2019 on the agreement between CSIRT GOV and CSIRT NASK regarding the delegation of duties.⁴⁰

References

- Banaśiński C, Nowak W (2018) Europejski i krajowy system cyberbezpieczeństwa. In: Cyberbezpieczeństwo. Zarys wykładu, Warsaw
- Chałubińska-Jentkiewicz K, Karpiuk M, Kostrubiec J (2021) The legal status of public entities in the field of cybersecurity in Poland. Lex Localis Press, Maribor
- Cilak M (2020) Komentarz do art. 9. In: Ofiarski Z (ed) Ustawa o finansach publicznych. Komentarz, LEX/el
- Lipiec-Warzech a L (2011) Ustawa o finansach publicznych. Komentarz, Warsaw
- Radoniewicz F (2019) In: Kitler W, Taczowska-Olszewska J, Radoniewicz F (eds) Ustawa o krajowym systemie cyberbezpieczeństwa. Warsaw, Komentarz
- Trąbiński P (2018) Podział kompetencji w zapewnianiu cyberbezpieczeństwa. In: Szpor G, Gryszczyńska A (eds) Internet. Strategie bezpieczeństwa, Warsaw

³⁷Communication No. 2 of the Head of the Internal Security Agency of 28 November 2019 regarding the conclusion of an agreement on the delegation of duties related to incidents reported by the Research and Academic Computer Network—National Research Institute Official Journal of the Internal Security Agency of 2019, item 22.

³⁸Communication No. 3 of the Head of the Internal Security Agency of 28 November 2019 regarding the conclusion of an agreement on the delegation of duties related to incidents reported by companies being members of the Capital Group of PGE Polska Grupa Energetyczna S.A Official Journal of the Internal Security Agency of 2019, item 23.

³⁹Resolution No. 125 of the Council of Ministers of 22 October 2019 on the National Policy Frameworks on Cybersecurity of the Republic of Poland for 2019–2024 Official Gazette of the Government of the Republic of Poland of 2019, item 1037.

⁴⁰The Communication of the Minister of Digitisation of 19 September 2019 on the agreement between CSIRT GOV and CSIRT NASK regarding the delegation of duties Official Journal of the Ministry of Digital Affairs of 2019, item 26.

Filip Radoniewicz PhD; legal advisor; adjunct in the Department of Cybersecurity Law and New Technologies at the Institute of Law, War Studies University, Warsaw; expert at the Academic Centre for Cybersecurity Policy, (War Studies University) and in the Ministry of Justice; he worked as an assistant judge (in the Fourth Criminal and Sixth Penitentiary Department of the Regional Court in Lublin); graduate of post-graduate studies: “European Union Law” at the Jagiellonian University, “Human Rights and Freedoms”, co-organized by the Institute of Legal Sciences of the Polish Academy of Sciences and the Helsinki Foundation for Human Rights, and “Computer Network Administration” at the Lublin University of Technology; author or co-author of approximately fifty publications, mainly in the field of broadly understood criminal law, new technology law and human rights. Selected publications: F. Radoniewicz (2016) *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym/Criminal liability for hacking and other offences against computer data and information systems*, Wolters Kluwer, Warszawa; *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz /Act on the National Cybersecurity System. Commentary/* (2019) ed. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, CH. Beck, Warszawa.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.