CEER

Council of European Energy Regulators

Fostering energy markets, empowering **consumers**.

Cybersecurity Benchmark

Cybersecurity Work Stream

Ref: C19-CS-56-03
18 December 2019

Council of European Energy Regulators asbl
Cours Saint-Michel 30a, Box F – 1040 Brussels, Belgium
Arrondissement judiciaire de Bruxelles – RPM 0861.035.445

INFORMATION PAGE

Abstract

This document (C19-CS-56-03) provides an overview of the cybersecurity landscape in the CEER Member countries represented in the CEER Cybersecurity Work Stream (CS WS) for the year 2018*.

The table highlights the main jurisdictional aspects, as well as the status of cybersecurity in each national energy sector.

Target Audience

European Commission, energy suppliers, traders, gas/electricity customers, gas/electricity industry, consumer representative groups, network operators, Member States, academics, national regulatory authorities (NRAs) and other interested parties.

Keywords

Cybersecurity, Benchmark.

* Disclaimer: Information contained in the following benchmark table is valid upon the date provided (unless otherwise specified), any further developments are not noted here. Not all CEER Members are represented in the CS WS.

If you have any queries relating to this paper, please contact:
CEER Secretariat
Tel. +32 (0)2 788 73 30
Email: brussels@ceer.eu

Table 1 – CEER Cybersecurity Benchmark 2018

Legend: ✓– *Yes; X – No; - – No answer provided; n.a. – NRA prefers not to / NRA cannot provide this information now / information not available due to confidentiality reasons; i.p. – in progress*

Disclaimer: Information contained in the grey column of the benchmark table is valid upon the date provided (2018) and any further developments are not submitted.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
National Level																
1. Planning: In which year was the last national strategy on security of network and information systems approved?	2013 (update of strategy in preparation)	2015[1]	2018	2015[2]	2016	2018	2013 National Cyber Security Strategy 2018 Strategy for the security of network and information systems[3]	The National cyber Security Strategy 2019-2024 is currently under development	2017	2018[4]	2018	2015	2019	2015	2016	National Cybersecurity Strategy 2019

[1] Next strategy on security of network and information is going to be approved in 2020.
[2] Reinforced by cyber defence strategic review of 2018 http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/
[3] https://hirlevel.egov.hu/2019/01/13/magyarorszag-halozati-es-informacios-rendszerek-biztonsagara-vonatkozo-strategiaja/
[4] Strategy was approved by Government resolution: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
2. Planning: What is the current status of the implementation of the Directive on Security of Network and Information Systems (NIS)? (In terms of existing or future national laws)	Implemented by law in December 2018 and by-law in July 2019	Fully implemented into Czech law by The Act No 181/2014 Coll. on Cyber Security.	Fully implemented into Danish law	Transposed by law # 2018-133 of 26 February 2018 and decree # 2018-384 of 23 May 2018	National cybersecurity law referring to NIS-Directive needs already decided upon and implemented	NIS transported by national decree #3218 of 7 July 2018	Fully implemented in Hungarian legislative, first revision to be drafted 2020	The NIS Directive has been transposed into Irish Lay under S.I. 360, 2018	Transposed into national legislation (law-decree 65/2018)	The NIS Directive was implemented in 2018, but sub statutory legal implementation continues in 2019 [5]	Transposed into national law on May 28 2019	The NIS was implemented 17 October 2018 and the laws were in force 9 November 2018	Draft law implementing the directive was submitted for consultation in December 2018	National cyber security law referring to NIS-Directive is being prepared (a draft exists)	National Information Security law	NIS Directive transposed by Royal Decree-Law 12/2018, on the security of networks and information systems

[5] Main document, in which NIS Directive was transposed is the Cyber Security Law.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
3. Governance Are there any dedicated laws for different subsectors of the energy market? Specific references on electricity, gas, oil RES, if they exist).	No sector specific laws, but sector specific risk analysis and CERT	X	✓	-	-	(EU) Regulation No **994**/2010 Security of supply of natural gas [6]	Electricity sector ES - NIS directive integrated into CIP Derivative energy markets – information security [7] legislative (Cobit based) [8]	The S.I. 360(2018) covers all sectors.	X	n.a.	X	Yes, there is an Electricity law, Gas law	-	-	X	There is only a general law Royal Decree-Law 12/2018, on the security of networks and information systems [9]

[6] Council Directive 2004/67/EC (3) **Pres. Decree 39/2011** (adjustment of EU Directive **EC 2008/114)** regarding the definition of European Critical Infrastructure Protection, *currently in force – general, not energy specific*

[7] https://net.jogtar.hu/jogszabaly?docid=a1300360.kor

[8] https://net.jogtar.hu/jogszabaly?docid=a1500042.kor

[9] A Draft Royal Decree implementing Royal Decree 12/2018, of September 7, on the security of networks and information systems is under way.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
4. Governance How many and which are the national competent authorities on security of network and information systems designated in your country? (references to any specific tasks).	Federal Chancellary (strategic tasks) and Ministry of Internal Affairs (operational tasks)	More than one	More than one	One	More than one	More than one *not energy specific*	Institute for Cyber Defence[10]	The National Cyber Security Centre is the designated authority	More than one. For energy and telecom, Ministry of Economic Development.	More than one (3 main institutions: 1.National Cyber Security Centre 2.State data protection inspectorate 3. Police department) [11]	"Institut Luxembourgeois de Régulation" and "Commission de Surveillance du Secteur Financier"	More than one	More than one	National Cyber Security Centre	More than one	Article 9. (Royal Decree-Law 12/2018, on the security of networks and information systems) [12]

[10] https://nki.gov.hu/

[11] Article: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr

[12] The following are competent authorities for the security of networks and information systems:
(a) For essential service operators:
- In the event that they are also designated as critical operators in accordance with Law 8/2011 of 28 April and their implementing regulations, irrespective of the strategic sector in which such designation is made: the Secretariat of State for Security, the Ministry of the Interior, through the National Center for the Protection of Infrastructure and Cybersecurity (CNPIC).
- In the event that they are not critical operators: the relevant sectoral authority on account of the subject matter, as determined by regulation.
b) For digital service providers: the Secretary of State for Digital Advancement, Ministry of Economy and Business.
c) For operators of essential services and digital service providers who are not critical operators falling within the scope of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector: the Ministry of Defense, through the National Cryptological Center. The National Security Council, through its specialized committee on cybersecurity, shall establish the necessary mechanisms for the coordination of the actions of the competent authorities.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
5. Governance Is there an entity which serves as the national single point of contact appointed? If yes, which is the designated Authority?	Ministry of Internal Affairs (receives information about incidents by CERT)	National Cyber and Information Security Agency (NÚKIB)	Center for Cybersikkerhed CFCS	ANSSI	Bundesamt für Sicherheit in der Informationstechnik (BSI)	n.a.	Institute for Cyber Defence[13]	The CSIRT which is part of the NCSC is the single point of contact for reporting NIS incidents. [14]	National Security Agency	National Cyber Security Centre[15]	Institut Luxembourgeois de Régulation	Minister van Veiligheid en Justitie (draft)	n.a.	National Cyber Security Centre	SI-CERT	Yes. National Center for Infrastructure Protection and Cybersecurity (CNPIC)

[13] https://nki.gov.hu/

[14] There is a NIS Compliance team within the NCSC. While the Compliance Team and the CSIRT are both within the NCSC, they are separate teams.

[15] Article 8: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
6. Awareness: Is a periodic status report on the state of cyber-security/IT-security published by the CERT/ CSIRT or a national agency?	✓	✓	Yes, Semi-yearly report by CFCS	✓	✓	X	✓	The CSIRT report a weekly report and a quarterly Threat Intel Landscape report	✓	✓[16]	✓	✓	✓	✓	✓	ANNUAL REPORT CCN-CERT-CIBERSECURITY (report 2018)
7. Governance Is a list of criteria to define Operators of Essential Services currently available?	Yes, published in a by-law in July 2019	✓[17]	✓	(cf. article 2 of decree # 2018-384 of 23th may 2018)	✓	✓	✓	Criteria are defined but not published	List of OESs exists but is not public (State secret)	✓[18]	Criteria are defined but not public.	✓	✓	✓	Decree determining essential services and the methodology for determining OESs	Relationship of essential services and number of Operators of Essential Services

[16] Last one was published in 2019: https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf

[17] The Decree No 437/2017 Coll. on the criteria for the determination of an operator of essential service.

[18] List of criteria is publicly available. (in methodology): https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
8. Awareness: Are there specific university educational programs, or any other educational tracks / cyber exercises in your country and by which academic institutions are organised/ conducted?	✓	✓	X	✓	✓	MSc in Cybersecurity (International Hellenic University) MSc Specialisation in Cybersecurity (University of Western Attica) [19]	✓	n.a.	ARERA is not involved in any educational programs	✓[20]	✓	X	✓	✓	✓	n.a.

[19] To be operating in academic year 2020-2021.
[20] Kaunas University of Technology (KTU), Vilnius University (VU), Vilnius Gediminas Technical University (VGTU), Mykolas Romeris University MRU (only CS management level).

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
9. Control: Is a certification according to any of the ISO/IEC27000 series standards available?	✓	✓	✓	X	✓	X	✓	The National Standards Authority of Ireland (NSAI) offer ISO27000 certification	✓	✓	✓	✓	✓	✓	✓	13/10/16 Resolution, Secretary of State for Public Administrations, approving the Technical Security Instruction
Energy Sector Level																
10. Planning: Are Operators of Essential Services in the energy sector identified?	In principle decided, operators receive formal information in October 2019	✓	✓	✓	✓	i.p.	✓	✓	✓	✓ [21]	Based upon predefined criteria, the identification of OES is ongoing.	✓	X	✓	X	✓[22]

[21] Critical infrastructure sectors (and Authorities/owners), including energy sector, are listed in appendix of critical infrastructure identification methodology: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e16e7761fc4b11e89b04a534c5aaf5ce?jfwid=q8i88m9wc. Detail list of critical infrastructure and owners is classified (restricted) information.

[22] Recognised, by National Center for Infrastructure Protection and Cybersecurity (CNPIC).

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
11. Assessment How many Operators of Essential Services in the energy sector do you expect to be defined in your country?	Approximately 50 (36 electricity, 7 gas, plus oil)	Approximately 15	Based on metrics	20 information may not be accurate	100 Information may not be accurate	n.a.	Around 10	Currently there are 10 defined	Around 50	n.a.	Based upon predefined criteria, the identification of OES is ongoing.	10 entities, 17 designations (7 DSOs do both gas and electricity).[23]	n.a.	12	n.a.	Essential service operators are 132, but we do not know the distribution by sector

[23] The change from 11 to 10 is because of 1 DSO was bought by another.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
12. Information Sharing and Emergency Response: Are Operators of Essential Services in the energy sector obliged to report critical security of network and information systems incidents? If yes, to whom?	NRA-Energy-Control Austria and Ministry of Interior as SPoC	✓They are obliged to report to gov CERT	Energinet (Danish TSO) and Center for Cybersikkerhed through a website	ANSSI	To BSI, and the BSI has to inform the NRA	National CERT optional	Institute for Cyber Defence[24]	Within the NCSC the CSIRT is the single point of contact for reporting NIS incidents. [25]	✓	National Cyber Security Centre	Institut Luxembourgeois de Régulation	✓	The Norwegian Water Resources and Energy Directorate	National Cyber Security Centre	SI-CERT	Yes, they should report to the CCN -CERT (Art. 19 Royal-decree law)

[24] https://nki.gov.hu/

[25] Upon receipt of a NIS incident notification, the CSIRT will notify the NIS Compliance team. While the Compliance Team and the CSIRT are both within the NCSC, they are separate teams.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
13. Planning: Are Digital Service Providers in the energy sector identified?	n.a.	X	X	X	X	i.p.	X[26]	X[27]	n.a.	n.a.	n.a.	X	n.a.	X	Exclusively critical Infrastructure Providers	n.a.
14. Planning: Does a dedicated strategy on security of network and information systems for the energy sector (or only for electricity or gas subsectors) exist?	National strategy with energy as subsector included	X	✓	X	✓	(EU) Regulation No **994**/2010 Security of supply of natural gas[28]	✓	The National Cyber Security Strategy was published in 2015.[29]	X	The National Cyber Security Strategy (NCSS) (published in 2018.[30]	X	X	X	-	X	National Energy Security Strategy

[26] Dgital service providers effecting energy sectors (cross-sectorial effects) are identified
[27] Within the NIS directive a 'digital service' is defined as: An online marketplace - An online search engine - A Cloud computing service.
[28] Council Directive 2004/67/EC (3) established a legal framework at Community level to safeguard security of gas supply in the case of supply disruptions.
[29] This is a cross-sectoral strategy which encompasses energy, finance, telcos, etc. Strategy for 2019-2024 will be published soon and will also be cross-sectoral.
[30] In 2019 was published inter-institutional action plan, which covers several sectors, including energy.
NCSS: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr
Plan:https://eseimas.lrs.lt/portal/legalAct/lt/TAD/faeb5eb4a6c811e9aab6d8dd69c6da66?jfwid=dg8d31595

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
15. Assessment Has an energy sector-wide security of network and information systems risk assessment been performed at national level?	Yes, performed in a Public Private Dialogue (PPD) process	X	✓	✓	✓	✓	A risk assessment was conducted in 2019 by the NRA regarding NIS directive	A risk assessment was conducted in 2014 across relevant stakeholders	There is a private forum discussing it	n.a.	X	X	✓	X	X	n.a.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
16. Assessment If such a risk assessment was made, does it include assessment of dependencies from surrounding countries, or any scenario which may derive from the existing market rules which would involve Member States, other than yours?	Indirectly yes because IT-companies are involved	n.a.	X	X	n.a.	Regulation (EU) No 994/2010, Provisions aimed at safeguarding the security of gas supply [31]	Yes. Risk assessment encompasses dependencies with EnC CPs (Serbia, Ukraine)	Yes. Risk assessment encompasses dependencies with Great Britain.	n.a.	n.a.	n.a.	-	X	-	n.a.	n.a.

[31] Designation of the "Competent Authority' by each Member State to be responsible for ensuring the implementation of the measures set out in this Regulation RAE has been designated as the Competent Authority, (article 12 L.4001/2011 ,FEK A' 179, 22.08.2011) Elaboration of Risk Assessment Establishment of a Preventive Action Plan and an Emergency Plan, and the regular monitoring of security of gas supply at national level.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
17. Governance Does the national regulatory authority have dedicated and trained executive officers, with expertise in security of network and information systems (any foresight for that)?	but limited resources	✓	✓	X	X	i.p.	✓	✓	X	X	✓	It is part of the NIS implementation	✓	✓	X	X

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
18. Information Sharing and Emergency Response: Does a dedicated sector-specific energy CERT/CSIRT or Essential Services CERT covering the energy sector exist?	✓	Covered by govCERT	X	Covered by CERT-FR	✓	X	The national CSIRT covers all sectors	The national CSIRT covers all sectors	X	Covered by National Cyber Security Centre: CERT.lt[32]	Covered by national CSIRT network	✓	✓	✓	X	✓[33]

[32] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Lithuania

[33] Article 11. Reference computer security incident response teams. (Royal Decree-Law 12/2018, on the security of networks and information systems)
These are reference computer security incident response teams (CSIRTs) for network and information system security, as follows:
(a) With regard to relations with essential service operators:
The CCN-CERT, of the National Cytological Center, which corresponds to the reference community constituted by the entities of the subjective scope of application of Law 40/2015, of October 1.
INCIBE-CERT, of the National Institute of Cybersecurity of Spain, which is the responsibility of the reference community constituted by those entities not included in the subjective scope of application of Law 40/2015, of October 1.
INCIBE-CERT will be jointly operated by INCIBE and National Center for Infrastructure Protection and Cybersecurity in all matters relating to the management of incidents affecting critical operators.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
19. Governance Is your regulatory authority in charge of any duty in relationship to the role of CSIRT/CERT in the scope of the energy sector?	✓	✓	n.a.	X	✓	X	E-ISAC.HU, NRA is in charge	n.a.	X	X	✓	X	X	X	X	National Center for Infrastructure Protection and Cybersecurity is in charge

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
20. Information Sharing and Emergency Response: Are national regulatory authorities informed in a timely manner about network security and information systems incidents through an institutional, even maybe an automated, mechanism ?	✓	✓	✓	X	✓	X	✓	n.a.	X	X	✓	n.a	X	✓	X	✓

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
21. Awareness: Have any security of network and information systems exercises been performed by the regulated energy companies? If yes, are there any OSEs as participants and who.	✓	✓	X	✓	✓	TSOs - DSOs - GRID Operators	✓	n.a.	main grid operators	n.a.	n.a.	✓	✓	✓	X	n.a.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
22. Governance Have the regulated energy companies – by requirement or not – implemented baseline security of network and information systems standards?	Sector specific security standards are in preparation by the sector, to be finished till end of 2019	✓	X	✓	✓	✓	main grid operators	n.a.	main grid operators	n.a.	✓	✓	✓	✓	✓	n.a.
23 Control: Has security of network and information systems been included in the audit plans of regulated energy companies (i.e. security audits)?	Is an obliged part of NIS-Directive	✓	✓	✓	✓	✓	✓	The NCSC will be auditing designated energy companies CRU may also include such audits	n.a.	n.a.	n.a	✓	✓	✓	Certified stakeholders (limited scope)	n.a.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
24. Governance Does an official national emergency plan exist that engages all stakeholders from private and public sector, in case of a crisis? if yes please refer to any designated National laws.	Depending on the manner of crisis: If sector overlapping impacts then there is a state catastrophe and crisis plan (SKKM), obligation by law for the Ministry of Internal Affairs	✓	✓	✓	✓	Regulation (EU) No 994/2010 Concerning measures to safeguard security of gas supply[34]	✓	n.a.	n.a.	✓[35]	✓	X	n.a.	n.a.	Critical Infrastructure Act	✓ [36]

[34] Aims at demonstrating all necessary measures are being taken to ensure continuous supply, in case of difficult climatic conditions, in the event of disruption (EU) Regulation Competent Authority RAE (article 12 L.4001/2011, FEK A' 179, 22.08.2011).
[35] https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.384076/asr
[36] National Center for Infrastructure Protection and Cybersecurity (PNPIC).

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
25. Awareness: Are there any cyber-security awareness campaigns/ forums/work shops, organised by a National Competent Authority or the Energy Regulator, engaging stakehol-ders of the energy sector?	Manifold activities, sector specific (organised by E-Control) and various platforms	Many activities, for example CyberCon (conference), cybersecurity exercise etc.	✓	in preparation	✓	Hellenic Center for Security Studies Military Cyber-Incident Response Center (Cyber Defense Directorate)	ENISA ECSM from 2016 every year		X	n.a.	in preparation	✓	✓	✓	✓	n.a.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
26 Control: Does a national or private or energy sector-specific laboratory test exist to verify the security and safety of software/ hardware components ?	Is in preparation by the Austrian Energy CERT (AEC, is the sector specific CERT)	X	X	✓	in preparation	X	in preparation	n.a.	n.a.	Planned (R&D division is established in National Cyber Security Centre it will cover all Critical infrastructure (owners)	X	n.a	X	X	in preparation (national)	There is no specific laboratory test for energy sector [37]

[37] National Cryptological Center acts as a certification body for Evaluation and Certification of Information Technology Security, applicable to related products and systems.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
27. Information Sharing: Does a voluntary collaborative platform for companies of the energy sector and the public sector to facilitate information sharing/best practices exist?	Voluntary information of incidents is also possible to the CERT	✓	✓	✓	✓	Gas Coordination Group [38]	✓[39]	Informal and voluntary arrangements are in place for information sharing	✓	n.a.	Regular cooperation in diverse working groups	✓	✓	✓	✓	For the public sector, National Cryptological Center shares guides and best practices [40]

[38] A platform to exchange information between MSs, the Commission, the gas industry and consumers.
[39] https://www.e-isac.hu/
[40] We don't know if there is something similar specifically for energy sector.

Issue	Austria	Czech Republic	Denmark	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Luxembourg	Netherlands	Norway	Portugal	Slovenia	Spain
28. Information Sharing: How many security incidents have been detected in the energy sector during the last 12 months?	n.a.	n.a.	information not available due to confidentiality reasons.	n.a.	n.a.	n.a.	approx. 12[41]	n.a.	11% of total number of attacks [42]	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	722 incidents over operators of Essential Services [43]

[41] Based on www.e-isac.hu anonymized data – official information not available due to confindentality reasons
[42] Source: Report on CS, sent to the Parliament by the National Security Agency.
[43] Data from national security annual report, but not only in the energy sector.

Annex 1 - List of abbreviations

Term	Definition
AMI	Advanced Metering Infrastructure
ANSSI	French Network and Information Security Agency
BATs	Best Available Technics
BREF	Best Available Technics reference document
CAPEX	Capital expenditure
CEER	Council of European Energy Regulators
CERT	Computer Emergency Response Team
CS WS	Cybersecurity Work Stream
CSIRT	Computer Security Incident Response Team
DG Energy	Directorate-General for Energy
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DSO	Distribution System Operator
EC SG TF EG	European Commission Smart Grids Task Force Expert Group
EEA	European Economic Area
EECSP	European Energy Cyber Security Platform
EFTA	European Free Trade Association
ENISA	European Union Agency for Network and Information Security
EU	European Union
Europol	European Union Agency for Law Enforcement Cooperation
Exploit	Software of set of commands taking advantage of a bug or vulnerability to cause unintended behaviour
GDPR	General Data Protection Regulation
GGP	Guidelines of Good Practice
Hack	To break into computers and computer networks
ICT	Information and Communications Technology
ID number	Identity number
IoT	Internet of Things
Malware	Hostile or intrusive software
MO	Metering Operator
MS	Member State (of the European Union)
Nation-state	Political entity on a territory coinciding with its citizens
NISD	Directive concerning measures for a high common level of security of Network and Information Systems across the Union
NRA	National Regulatory Authority
OES	Operators of Essential Services
OPEX	Operational expenditure

Term	Definition
REMIT	Regulation (EU) No 1227/2011 of the European Parliament and of the Council on wholesale energy market integrity and transparency
SCADA	Supervisory Control and Data Acquisition
SGO	Smart Grid Operator
SO	System Operator
Trojan	Malicious computer program misleading users of its true intent
TSO	Transmission System Operator
Wiper	Malware with the aim to wipe the hard drive of the computer it infects
Worm	Malicious computer program that replicates itself to spread to other computers

Annex 2 – About CEER

The Council of European Energy Regulators (CEER) is the voice of Europe's national energy regulators. CEER's members and observers comprise 39 national energy regulatory authorities (NRAs) from across Europe.

CEER is legally established as a not-for-profit association under Belgian law, with a small Secretariat based in Brussels to assist the organisation.

CEER supports its NRA members/observers in their responsibilities, sharing experience and developing regulatory capacity and best practices. It does so by facilitating expert working group meetings, hosting workshops and events, supporting the development and publication of regulatory papers, and through an in-house Training Academy. Through CEER, European NRAs cooperate and develop common position papers, advice and forward-thinking recommendations to improve the electricity and gas markets for the benefit of consumers and businesses.

In terms of policy, CEER actively promotes an investment friendly, harmonised regulatory environment and the consistent application of existing EU legislation. A key objective of CEER is to facilitate the creation of a single, competitive, efficient and sustainable Internal Energy Market in Europe that works in the consumer interest.

Specifically, CEER deals with a range of energy regulatory issues including wholesale and retail markets; consumer issues; distribution networks; smart grids; flexibility; sustainability; and international cooperation.

CEER wishes to thank in particular the following regulatory experts for their work in preparing this report: Leontini Kaffetzaki, Roman Picard, Stefano Bracco and special thanks to Liselotte Gijzemijter.

More information is available at www.ceer.eu.