EUROPEAN
COMMISSION

Brussels, 3.4.2019
SWD(2019) 1240 final

COMMISSION STAFF WORKING DOCUMENT
Accompanying the document

Commission Recommendation

on cybersecurity in the energy sector

{C(2019) 2400 final}

1. INTRODUCTION

The energy infrastructure is one of the most critical assets for a modern society. Its effective operation is a pre-condition for securing energy supply to a wide range of economic and social activities and thus enables societal welfare and stability. Due to the over-arching need to tackle climate change and the necessary transition to a low-carbon economy as well as the rapidly increasing digitalisation, the energy sector is undergoing a very rapid transformation in terms of infrastructure and market functioning. An additional factor that stimulates changes in the sector is the active participation of citizens in the energy market as consumers and decentralised producers of energy.

Traditional energy technologies, which are historically composed of control systems specifically tailored to operate the physical networks, are being more and more connected to modern, digital technologies and components. The advancing digitalisation makes the energy system smart and enables consumers to actively participate in the energy market and to better benefit from energy services. At the same time, digitalisation creates risks by an increased exposure to cyber-attacks and cybersecurity incidents jeopardizing the security of supply or the data privacy of consumers.

Cybersecurity incidents and cyber-attacks in the energy sector could have devastating and wide-ranging impacts. The European energy sector is characterised by numerous physical interconnections in electricity, gas and oil and is increasingly witnessing electricity and gas market coupling. In view of such increased interdependencies, the cascading effects that can be the consequence of a cyber-attack may potentially affect not only several sectors in one Member State but also produce considerable damage across critical infrastructures and energy sectors in a number of other Member States.

Cyber-attacks addressing the energy system are a reality today and have a long history reaching back to 1982 when malware was introduced into SCADA systems triggered an explosion of a gas pipeline in Siberia. In 2010, the Stuxnet cyber-attack on Iranian nuclear installations constituted the first known autonomous threat to target and sabotage industrial control systems to such an extent. On 23 December 2015, nearly 225.000 customers in three areas of Ukraine endured hours of blackout due to a cyber-attack on the control system of a power grid. In 2017, threat actors targeted US government entities and the energy, water, aviation, nuclear and critical manufacturing sectors.

At this stage the Commission does not dispose of any specific and clear indication that an attack of a certain magnitude might be imminent. However, taking into account both the risks of such occurrence as well as its potential impact on European level, the Commission considers that all Member States and energy stakeholders should be properly prepared. Therefore, for the first time the Commission has elaborated a

Recommendation on cybersecurity in the energy sector[1] containing a set of guidelines that should help Member States and stakeholders concerned cope better with this new security challenge.
This Staff Working Document accompanies the Commission Recommendation. It aims at providing additional information and background on cybersecurity in the energy sector on the following aspects:

- The policy context
- The characteristics of the energy sector requiring a specific approach on cybersecurity
- The on-going relevant Commission fora and activities
- The relevant international standards

2. POLICY CONTEXT

A comprehensive approach to energy security, including cyber security has gained significant importance in the European energy policy over the last years. This resulted in declaring security as one of the five dimensions of the Energy Union. The Energy Union Strategy[2], adopted by the European Commission in 2015, specified that security is an indispensable feature of the energy system of the future. This policy orientation was quickly translated into new legislative proposals by the Commission.

2.1. Energy

Delivering on the Energy Union goals requires a fundamental transformation of Europe's energy system while maintaining a high level of security. The adoption of all eight legislative proposals of the Clean Energy for All Europeans[3] package paves the way for the EU to lead the clean energy transition and creates an optimal environment for taking advantage of the digital transformation in the energy sector. With variable power generation becoming a main feature of the market and with more interconnections and opportunities through digitalisation, an updated design of the electricity market was needed. The package introduces a new regulatory framework for more flexible and better co-ordinated energy markets and takes account of recent developments in areas such as smart grid, digitalisation and cybersecurity. The recast of the Regulation on the internal market for electricity[4] provides a legal basis for the adoption of future technical rules for electricity such as a Network Code on Cyber Security.

---

1 C(2019) 2400

2 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy, COM/2015/080 final.

3 Directive (EU) 2018/2001; Directive (EU) 2018/2002; Regulation (EU) 2018/1999; Directive (EU) 2018/844. The European Parliament confirmed the political agreements reached with the Council on Electricity Market Design proposals (Risk-Preparedness Regulation, Regulation for the Agency for the Cooperation of Energy Regulators (ACER) and the Electricity Directive and the Electricity Regulation at the plenary session of March 2019. The Council formal adoption is expected to take place in April; the publication of the legal text in the OJ will follow soon thereafter.

4 COM/2016/0861

Another legislation in the Clean Energy Package that addresses cybersecurity is the Regulation on Risk Preparedness[5]. According to this Regulation, crisis scenarios must be identified at national and regional level on the basis of, at least, a set of risks explicitly including cybersecurity. These crisis scenarios are the basis for Member States to draw-up Risk-Preparedness Plans to ensure optimum preparedness for electricity crises and an effective management of such situations should they occur.

Risk-Preparedness Plans should consist of two parts, setting out national measures and coordinated measures agreed between the Member States in a region. They should take into account the specific characteristics of each Member State and set out clearly the roles and responsibilities of the competent authorities. Measures to ensure that simultaneous crises are properly prevented and managed must be part of the Plans.

The Regulation also includes obligations for Member States to inform neighbouring Member States and the Commission without delay in the event of a crisis.

In the case of gas, the main legal act is the Regulation on Security of Gas Supply. According to the Regulation, Member States have to consider cyber-attacks as part of the risks to the secure supply of gas at national and regional level. All those risks, including cyber security, must be considered in national Risk Assessments that all Member States have to prepare every four years. Moreover, such national Risk Assessments are accompanied by a set of common Risk Assessments jointly developed by groups of Member States that share a certain source or route of gas supply[6]. Cybersecurity must also be considered in these common Risk Assessments.

On the basis of the results of the national and regional Risk Assessments, Member States have to adopt a Preventive Action Plan containing the necessary preventive measures to address those risks identified as relevant for each Member State. Member States must also develop joint measures to address the risks identified at regional level. Similarly, Member States must adopt an Emergency Plan describing the measures, procedures and actors to mitigate the impacts of a potential gas crisis at national and regional level. Such emergency measures cover the necessary technical measures to remedy the cause of the crisis as well as broader contingency measures, such as alternative supply measures and selective demand curtailment. In the design of such measures it is important to give due consideration to the nature and origin of the crisis and the particularities that may emerge thereof. Appropriate communication channels in the case of a crisis must also be established within the Member State, with other Member States potentially affected and with the Commission.

5 COM/2016/0862

6 Annex I of Regulation (EU) 2017/1938 defines the groups of Member States.

2.2. Cybersecurity

This energy specific sectorial approach is based on the general European policy on cyber security. The importance of cyber security was strategically fully recognised for the first time at EU level with the adoption of the EU Cyber Security Strategy in 2013[7]. The adoption of the Directive on security of network and information systems[8] (Directive (EU) 2016/1148) in July 2016 was a key step towards establishing cyber security resilience at the European level. This Directive sets the first EU-wide rules on cybersecurity, improves cybersecurity capabilities and strengthens cooperation between Member States. It also requires companies in critical sectors, such as energy, to take appropriate security measures and to notify any serious cyber incident to the relevant national authority.

Consistent implementation of this "NIS" Directive across different sectors and Member States is provided by the NIS Cooperation Group, which was established under Article 11 of the Directive and is tasked with enhancing cooperation between competent authorities for the NIS Directive. The Cooperation Group, which started its work in February 2017, facilitates sharing of national experiences and exchange of best practices with a view to ensuring a high level of security while reducing the risk of market fragmentation.

The Cooperation Group committed through its first biennial Work Programme (2018-2020) to investigate sector-specific aspects influencing the implementation of the NIS Directive and, ultimately, affecting the cyber-resilience of certain sectors. In this context, the Group decided to establish a dedicated work stream on cybersecurity in the energy sector in 2018. Such work stream enables an in-depth discussion concerning the implementation of the NIS Directive and should lead to the spread of good practices amongst the relevant players.

Further, the NIS Directive establishes in Article 12 the operational CSIRTs Network[9]. The CSIRTs Network is a network composed of EU Member States' appointed CSIRTs and of CERT-EU with the aim to develop confidence and trust between the Member States and to promote a swift and effective operational cooperation. The European Commission participates in the network as an observer. The European Network and Information Security Agency ENISA is tasked to actively support the CSIRTs cooperation, and to provide the secretariat and active support for incident coordination upon request.

---

7 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7.2.2013, JOIN(2013)1.

8 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1.

9 https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

On 13 September 2017, the Commission adopted a Cybersecurity Package. The Joint Communication on Cybersecurity[10] of this Package acknowledges the importance of sector-specific considerations and requirements at EU level, including in the energy sector. Also part of this Package was the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises[11]. This "Blueprint for rapid emergency response" sets out the objectives and modes of cooperation between Member States and EU Institutions in responding to large scale cross-border cyber incidents or crisis.

The Cybersecurity Act[12], which was also part of the Cybersecurity Package of 2017, reinforces the mandate of the EU Agency for Cybersecurity so as to better support Member States in tackling cybersecurity threats and attacks. The Cybersecurity Act also creates a framework for European Cybersecurity Certificates for products, processes and services that will be valid throughout the EU and is of particular interest for the energy sector.

2.3. Critical Infrastructure

Reducing the vulnerabilities of critical infrastructure and increasing their resilience has been one of the major objectives of the EU since the launch of the European Programme for Critical Infrastructure Protection (EPCIP). In its EPCIP Communication[13] of December 2006, the Commission sets the overall framework for activities aimed at improving the protection of critical infrastructure in Europe, across Member States and in all relevant sectors of economic activity. An important pillar of this programme is the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection[14]. It establishes a procedure for identifying and designating European Critical Infrastructures (ECI) in the energy and transport sector as well as a common approach for assessing the need to improve their protection. The Directive requires owners/operators of designated ECI to prepare Operator Security Plans (advanced business continuity plans) and nominate Security Liaison Officers (linking the owner/operator with the national authority responsible for critical infrastructure protection). All Member States transposed the directive; however its review conducted by the Commission in 2012 concluded that the real results achieved were limited. Some Member States designated many ECIs, some others did not register any. Following the

10 Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 13.9.2017, JOIN(2017) 450 final

11 C(2017)6100/F1

12 The Cybersecurity Act was adopted by the European Parliament in March 2019. The Council formal adoption is expected to take place in April; the publication of the legal text in the OJ will follow soon thereafter.

13 Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 of 12.12.2006.

14 OJ L 345, 23.12.2008, p. 75.

evaluation, the Commission[15] proposed in its Staff Working Document a new, more hands-on approach on EPCIP. The new approach focuses at interdependencies between sectors and between Member States. In this context, four critical infrastructures of a European dimension – Eurocontrol, Galileo, the electricity transmission grid and the gas transmission network – were selected in order to optimise their protection and resilience.
In the context of the implementation of the ECI Directive in the energy sector, the Directorate-General for Energy of the European Commission started the Thematic Network on Critical Energy Infrastructure Protection (TNCEIP) in December 2010. The TNCEIP provided to energy operators a platform for the exchange of knowledge and experiences on the subject of critical infrastructure protection. It also helped the members profit from information exchange regarding the security of critical and large-scale energy facilities and infrastructures, including important related subjects of trans-national dimension, the latest academic research and lessons learned from experiences in the EU, and national or regional initiatives.

The protection of energy infrastructure and issues related to cybersecurity are also of particular importance in the context of countering new types of threats. In April 2016, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy adopted a Joint Framework[16] to counter hybrid threats and foster the resilience of the EU, its Member States and partner countries while increasing cooperation with NATO on countering these threats. The Joint Framework brings together existing policies and proposes twenty-two operational actions aimed among others at raising awareness and building resilience by addressing potential strategic and critical sectors such as energy, transport and space. The Commission and the High Representative annually report[17] on progress achieved on the implementation of the Joint Framework on countering hybrid threats. In response, the European Council[18] highlighted the need to step up the capacity of the EU and its Member States to detect, prevent and respond to hybrid threats in areas such as cyber, strategic communication and counter-intelligence. Against this background, in June 2018 the Commission and the High Representative prepared the second report[19] on the implementation of the Joint Framework on Hybrid Threats focusing among others on cybersecurity.

The Commission, in close cooperation with the stakeholders, identified the following three specific characteristics of the energy sector as far as cybersecurity is concerned: cascading effects, real-time requirements and the need to jointly manage new and old

---

15 Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure, SWD (2013) 318 final of 28.03.2013, p. 7.

16 Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats a European Union response, JOIN/2016/018 final.

17 Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats - a European Union response, JOIN/2017/030 final.

18 European Council conclusions of March 2018.

19 Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats: Increasing resilience and bolstering capabilities to address hybrid threats, JOIN(2018) 16 final.

technologies. In May 2018, the Florence Forum[20] acknowledged these characteristics as key energy-specific cyber security challenges that require tailored cyber security approaches. These specific challenges cannot be fully addressed through approaches or solutions applied in other sectors. It is, therefore, indispensable to look at the particularities of the energy sector and propose solutions that will take account of the sectorial requirements and increase the overall level of cyber security among the stakeholders.

3. SPECIFICITIES OF THE ENERGY SECTOR AND POSSIBLE ACTIONS TO ADDRESS CYBERSECURITY CHALLENGES

3.1. Real-time requirements

Some energy systems (e.g. circuit breakers, turbine and protections devices) need to react very fast. For example, there are timing requirements for circuit breakers that go down to 3 milliseconds (ms) according to the international standard IEC 61850-5.

There are numerous examples of real-time requirements in the energy sector, which have not been designed to consider additional cybersecurity processing time. For example the time constraint for GOOSE messages between substations can go down to 10 ms. Also peer-to-peer messages inside a substation replacing hard wire can go down to 4 ms.

As a result, a number of common security measures, like the authentication of a message, cannot be incorporated using all degrees of freedom for the selection of the cryptographic mechanisms, because some mechanisms may introduce an unacceptable additional delay. For example, the international standard IEC 62351-6 Edition 1 defines security for GOOSE (switchgear measurement and control) utilizing digital signatures. This has been proven infeasible for the target environment, as the computation on the target devices would take too much time. Instead, practical implementations have shown that message authentication can be provided faster by using HMAC functions (like HMAC SHA256) or AES-GMAC[21]. This has been considered in Edition 2 of IEC 62351-6.

Securing communication channels where there are no time constraints is already manageable by current systems, but a special focus is required in those systems where a real-time reaction is necessary (processing and transmission time).

When introducing security, process requirements need to be considered in order not to hamper the performance of the system.

<u>Segregating of networks:</u>

[20] See conclusions of the 33rd Florence Forum of May 2018. More information on the Florence Forum can be found in Annex I.

[21] HMAC and AES-GMAC are specific types of message authentication code (MAC)

One possibility to better address the different time and process requirements in electrical systems is to split the overall system into logical zones and processes. This would allow operators to define time constraints per zone and process in order to assess the associated cybersecurity measures within each zone.

Secure communication and authentication:

The communication between an installation and its remote energy management system or distribution management system[22] needs to be properly secured and controlled. There are commercial protocols that allow for the consideration of such real-time requirement. The protocol chosen should be tested prior to its introduction and need to consider real-time requirements, as encryption and network control mechanisms always add a time overhead.

In addition to a secure communication, it is important to introduce proper authentication mechanisms, including machine-to-machine authentication and operator-to-machine authentication. A protocol that ensures secure communication but not appropriate authentication could also make an energy system vulnerable. In this regard, it is important to consider potential real-time requirements when introducing an authentication mechanism. For those network segments containing devices which are not supporting network security mechanisms (e.g. not supporting encryption), at least strict network access control mechanisms must be put in place.

Asset management through classification:

Nowadays, facilities contain a large quantity of assets. An asset is any data, device or service, which represents a value for the company and for its capability to deliver services. Operators should be well aware of all assets in their facilities. A classification scheme, including time and process constraints for these assets, should be introduced in order to allow for an efficient management, a fast response and maintenance/upgrade planning.

Public and private infrastructure:

From a security of design point of view, a private autonomous network within the facility is the optimal solution to protect communication and at the same time ensure the required level of quality-of-service regarding real-time constraints. However, due to cost implications, using a private network might not always be possible. Allocating capacity on public networks can then be an alternative, although public networks, or networks of third parties, pose certain risks. Using IP Sec (Internet Protocol Security, such as RFC6071), to virtually segregate and protect the company network flows in shared network scenarios has been proven to work well under near-to-real-time requirements, for example in grid automation, typically found in the distribution area and with real-time

[22] Energy Management System (EMS) - Distribution Management System (DMS).

constraints in milliseconds. Where IPSec is not supported, the use of other Virtual Private Network (VPN) and tunnelling solutions should be taken into consideration (including, if needed, those available in the upper layers of the OSI Stack).

Physical security & hardening of interfaces:

In general, peer-to-peer communication presents added complexity in terms of security implementation. Peer-to-peer real-time communications within substations should be secured according to the ongoing standardisation effort by working group 15 of TC57 on IEC 62351. Nowadays, there is still a lack of commercially available products implementing secure real-time communication protocols. Therefore, the interfaces between installations and any external network need to be strengthened and physical security of installations need to be ensured. Once standards are commercially available, they should be used.

If it is not possible to upgrade the installed base, complementary physical security is necessary. Besides the physical protection of the local substation automation communication network, best practices of network security like filtering or segmentation down to station level should be in place.

3.2. Cascading effects

Electricity grids and gas pipelines are strongly interconnected across Europe and well beyond EU Member States. A cyber-attack creating an outage in a part of the energy sector might trigger immediate and far-reaching cascading effects into other parts, regions or sectors.

On a power line, the electricity produced in one region does not have to pass any physical border before being consumed in a second region. Moreover, the stability of electricity supply depends on the integrity of the entire electricity grid in Europe and beyond. A sudden failure of a single transmission or distribution element in a power grid can induce a rapid domino effect of cascading failures, which can lead to the disruption of the supply of a large number of consumers or even to the failure of the entire or many parts of the European power grid. The most commonly known example of a cascading effect happened in 2006 after the planned shutdown of a high voltage line in Northern Germany that affected many European countries and millions of customers[23].

The cross-border miscommunication case of Austria and the German region of Bavaria in 2013[24]– even no cascading effect originated from it – is another incident that shows the interconnectivity of different sub-sectors as well as the connectivity between different countries. In this incident, a misleading control command in an Austrian power grid led

[23] Example of cascading effects, Germany November 2006: http://europa.eu/rapid/press-release_IP-07-110_en.htm?locale=en, 03/07/2018.

[24] EECSP report: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf (February 2017).

to broadcast that flooded the communication network similar to an ‘internal’ Denial-of-service (DoS) attack. This incident was resolved without any power outages.

Criticality and setting appropriate measures:

It is indispensable for asset owners to evaluate the criticality of their assets, i.e. the degree to which a failure in a concrete asset would have a severe impact in the network. This evaluation process should cover generation and flexible-demand systems, transmission and distribution substations and lines, as well as the associated impacted stakeholders in case of an attack. The interdependencies among the affected stakeholders should be taken into consideration and be analysed to identify the potential impacts of cyber-attacks and cybersecurity incidents. After identification of the criticality and the interdependencies, procedures to allow quick recovery after an attack should be defined.

Official certification or labelling schemes for cybersecurity may be considered, as well as after-sales re-certification processes. In this regard, it is recommended that purchased new devices be equipped to receive future patches, have ensured lifecycle support and that the vendors have in place after-sales product monitoring and patching (i.e. monitoring the presence of vulnerabilities and providing patches).

Considering possible cyber-physical spill-overs:

In terms of cybersecurity and cascading effects of the energy system, it is important to address cyber-physical effects. This concerns the damage of physical assets through a dedicated cyber-attack as well as broader effects affecting the security of supply of an area.

Thus, resilient grid design criteria, architecture and business continuity plans should be established and regularly reviewed to ensure that cyber-physical events are adequately considered.

Establishing design criteria and architecture for a resilient grid:

Depending on the criticality identified, appropriate security concepts, like defence-in-depth (multi-layered security approach), should be put in place per site in order to limit the impact and gain time in case of a cyber-attack or a cyber incident

The digital environment must be designed to mitigate the risk of cascading effects and to ensure the resilience of the system. This can be achieved by identifying critical nodes in the grid in terms of power production capacity and customer impact. Digital controls need to be designed to avoid being a single point of failure for several critical nodes or grids in case of simple component or device failures. Communication and control networks need to be designed with segmentation criteria that allow to limit physical and logical potential failures to a same part of the grid.

Having in place proper communication and cooperation:

Preventing cascading effects goes beyond the area of control of each operator, so appropriate communication and cooperation frameworks must be set up between relevant stakeholders. To ensure proper communication within an operator and also among operators, structured communication channels have to be in place, including a defined information classification scheme, processes on how to handle sensitive information and a defined structure of the information to be shared.

Additionally, a communication framework with key and impacted stakeholders should be introduced to share early warning signs. As a guiding principle, information flows between operators and authorities must be well established.

3.3. Legacy technology combined with new internet-of-things devices

The energy sector of today contains two different extremes of technology elements in its infrastructure. On the one hand, there is basic infrastructure, designed at a time well before cyber security considerations came into play and having a lifetime of 30-60 years. This legacy is not only about analogue technology but also – and more importantly – about digital technology designed prior to cyber-security considerations. On the other hand, there is more and more recent state-of-the-art equipment for automation and control, strongly supported by smart concepts and digital technologies connected to the basic infrastructure.

These new technologies are adding greater flexibility and control to accommodate distributed energy resources and electric vehicles and thus help adapt to the changing more flexible and distributed market environment. This digital revolution enables new services and business models for operators and serves at the same time to ensure greater reliability and security of supply. The energy sector therefore needs to find ways how to embark on an increasingly digitalised future without being compromised by its pre-cybersecurity legacy.

The number of Internet-of-Things (IoT) devices and applications related to the energy sector is growing rapidly. While the Internet-of-Things represents the next step towards the digitisation of our society and economy, where objects and people are interconnected through communication networks, report about their status and interact with the surrounding environment, it creates new challenges for the necessary balancing of the grid. New smart installations such as heating systems, air conditioners, electric water kettles, home automations, photovoltaic installations and electric vehicles can become a new cyber threat if maliciously controlled, which could trigger un-forecasted changes in demand and endanger the stability of the grid.

As many IoT systems are based on similar technologies or communications, a cyber-attack could exploit a common vulnerability for many units covering a wide area. This makes the introduction of IoT devices a threat to all actors in the energy system, no matter what size they are.

Each operator should therefore be aware of what is connected to the network, from photovoltaic installations to electric vehicles. While it is true that such task is becoming increasingly hard for operators given the increase of the number of devices "behind the meter", each operator should be prepared for the possible case of intensive network fluctuations due to a cyber-attack.

Establishing sufficient knowledge about the security of assets and infrastructure:

The energy sector requires some operational technologies (OT) that consist of both legacy and modern IT-based systems. This OT is gradually connected to a complex and highly interconnected digital environment – smart metering devices, 5G, Internet-of Things, sensors, electric vehicles, storage, distributed energy resources, sometimes using artificial intelligence and cloud-based solutions. It is therefore essential for operators to know the internal dependencies of their networks and services and to be aware about external interfaces and their vulnerabilities in terms of outbound and inbound damage propagation.

It is necessary to develop suitable measures against malicious attacks, such as distributed denial-of-service attacks against networks, originating from large numbers of maliciously controlled consumer devices or applications.

Operators should limit the use of IoT devices to operational needs and promote end-user cyber-security awareness campaigns. Each end-user using an application for e.g. home automation should be aware of the dangerous consequences of careless internet use. Basic cybersecurity hygiene, such as regular software updates, and secure password handling should be the usual practice.

Additionally, an automated monitoring and analysis capability for security related events, such as unsuccessful attempts to connect, door alarms for cabinet opening etc. should be introduced.

To mitigate cyber threats systematically, a risk-based approach is recommended. This comprises a business continuity management and risk management according to international standards or best practices, such as ISO 22301 or ISO/IEC 31000. Additionally, an Information Security Management System (ISMS) supports companies to manage information security risks as described for instance in the ISO/IEC 27000-family of standards (see more on standards in chapter 5)

Specific risk analysis:

Having these developments in mind, specific cybersecurity risk analyses on all legacy installations, focusing on external and internal attacks should be conducted on a regular basis and as part of the organization's risk management framework. The assessment should include mobile devices interfacing the system like USB, PC, tablet, etc. especially if access is performed for adjusting device settings or for upgrading.

Given that legacy installations often represent a very large number of assets, risk analysis might be done by asset category, and fine-tuned at a later stage. This recommendation assumes that there is some standardization between assets of a same type, which is true for the most recent and small installations. Larger plants are often the result of completely different projects, for historical reasons, and their "upgrades" have been quite frequently planned independently. Because of this, each installation is quite often rather unique, also in term of assets. This could limit the degree to which Risk analysis "by asset class" can be conducted.

Penetration testing and vulnerability assessments of legacy and new technologies could be conducted to understand risks related to legacy installations and to identify improvement opportunities. However, penetration testing has its limits as there are risks of damaging assets in production environments, thus test environments or simulated environments could be possible alternatives where systems in operation cannot be directly tested.

The risk in communication between facilities and control centres, with attacks possibly originating from the control centre, should also be assessed

Performing a systematic patch management and establishing alternative procedures where patch management is not possible:

Patches are a key element for all industrial systems to update software and to counter possible cyber-attacks. Systematic patch management is essential to facilitate system updates. Ideally, the patch management process should also include pre-production patch testing and rollback functionalities. Given that software and firmware used in facilities are quite often developed ad-hoc, it is important to test the effects of the patches before installing them in production systems. It is also important to be able to go back (rollback functionalities) if the patch, after application, made the system unstable.

There are constraints to patching related to the physical structure of the network. Deploying patches might require for example stopping the operational production. Thus patching might only be a solution in maintenance operations, which might only occur on a multiannual basis. Consequently, other alternatives should be considered, like reducing the risk of external intrusion through adding an external security barrier on top of the existing security mechanisms. Moreover, the segregation of an installation into several zones of different risk and criticality levels would be a step to increase security. For better monitoring and to be alerted of unsuccessful attempts to connect, the capability to retrieve information about cyber-events should be added.

An important point is to collaborate with technology providers (vendors) to replace legacy systems whenever beneficial for security reasons, but taking into account critical system functionalities.

Physical security:

Physical protections are an important measure to complement cybersecurity efforts to reinforce security of legacy systems and should be reviewed on a regular basis

Strengthening the security in the supply chain:

Operators and the European energy system are depending on technology providers. Every technology tender should address cyber security requirements and demand compliance with existing cyber security standards and security services. Technology tenders should also address the handling of new vulnerabilities.

The Cybersecurity Act[25] reinforces the mandate of the EU Agency for Cybersecurity, (ENISA) so as to better support Member States with tackling cybersecurity threats and attacks. The Act also establishes a European framework for cybersecurity certification, aimed at boosting the cybersecurity of ICT products, services and processes. In addition, Expert Group 2 of the Smart Grids Task Force[26] is working on how to address supply chain management in the upcoming network code on cybersecurity (Clean Energy for all Europeans Package). In their final report, the Expert Group links their proposal to the politically agreed version of the Cybersecurity Act.

4. OVERVIEW OF RELEVANT COMMISSION FORA AND ACTIVITIES ADDRESSING CYBERSECURITY IN ENERGY

In the past years, the Commission has initiated a number of fora to facilitate exchanges between experts and stakeholders to better address cybersecurity concerns and to broadly improve resilience in the energy sector. These actions[27] continuously feed into the efforts to spread good practices, promote policy developments and hereby increase the level of cybersecurity in the EU energy sector.

In December 2015, DG Energy created the Energy Expert Cyber Security Platform (EECSP) in cooperation with other services. Its purpose was precisely to analyse the specific needs of the energy sector in terms of cyber security. Based on its findings[28] and as a direct action following from the Clean Energy for All Europeans package, the European Commission set up a Stakeholder Working Group to focus on practical approaches and solutions to improve the resilience of the energy network in spring 2017. The group finalised its report and recommendations to the Commission early 2019.

DG Energy has taken a deeper look at the specificities of the energy sector and identified the three main particularities of the energy sector described in the Recommendation and in this SWD. These specificities were confirmed by stakeholders in a series of hearings

[25] The Cybersecurity Act was adopted by the European Parliament in March 2019. The Council formal adoption is expected to take place in April; the publication of the legal text in the OJ will follow soon thereafter.

[26] See Annex 2

[27] Annex I provides a more detailed overview of all actions and initiatives undertaken.

[28] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

that took place in February 2018. The 33rd Florence Forum[29] also confirmed in its meeting in May 2018 these specificities and called for guidance from the Commission.

Early 2018, DG Energy organised a series of stakeholder hearings to further investigate these particularities with all main stakeholders[30] relevant for the energy sector to get a better understanding of the concerns of the energy sector and how stakeholders see the role of the EU. The particularities of the energy sector that raise challenges in terms of cyber security were confirmed in these hearings.

In parallel, between April 2017 and May 2018, DG ENER asked the Conseil de Cooperation Economique (CCE) to take a deeper look at the particularities of the energy sector and to provide technical recommendations on EU guidelines for the energy sector. These recommendations differ from other recommendations related to cyber security as they are completely aligned with the three confirmed particularities of the energy sector.

The Commission is also working to raise awareness about cybersecurity and to promote broad discussions among different stakeholders from the energy sector. For this purpose, the Commission organised an event on cybersecurity in the energy sector in Rome in March 2017 on the occasion of the 60th anniversary of the Treaty of Rome. The outcome of this event fed into a dedicated G7 experts meeting on cyber security in the energy sector in Rome in 2017. In October 2018, the Commission invited to a high-level conference[31] dedicated to cybersecurity in energy, which around 200 interested participants attended. Additionally, small stakeholder workshops were organised to further discuss the particularities of the energy sector.

In addition to raising awareness, sharing information on cybersecurity and cyber resilience in the energy sector is another area of work for the Commission. The Commission aims at strengthening the position of the European Energy – Information Sharing Analysis Centre (EE-ISAC) as one of the formal follow-up actions to the Cybersecurity Package of 2017. The EE-ISAC helps utilities to improve the cybersecurity and resilience of their grid by enabling trust-based data and information sharing.

Finally, the first sectorial work stream of the NIS Cooperation Group, established under the NIS Directive, focuses on energy and held its kick-off meeting in June 2018. This

---

29 https://ec.europa.eu/energy/en/previous-editions-florence-forum

30 Stakeholders consulted include the European Network of Transmission System Operators for Electricity (ENTSO-E), the European Network of Transmission System Operators for Gas (ENTSO-G), the European Cybersecurity Organization (ECSO), CCE, the Union of the Electricity Industry (Eurelectric), The European gas association (Eurogas), the European association of electricity distribution system operators (EDSO), the Groupement Européen des entreprises et Organismes de Distribution d'Energie (GEODE) and the Commission Agencies ACER (Agency for the Co-operation of Energy Regulators) and ENISA (the European Union Agency for Network and Information Security Agency)

31 https://ec.europa.eu/info/events/cybersecurity-energy-sector-2018-oct-11_en

work stream shows that the specificities of different sectors are important when addressing cybersecurity, as recognized in the Cybersecurity Package adopted in September 2017.

Besides the energy sector, there are also other sectors like the transport or financial sector that are experiencing increasing digitalisation and are thus might be vulnerable to cybersecurity incidents and cyber-attacks. Therefore also other sectors address cybersecurity issues related to their respective particularities. For instance in the aviation sector, the European Commission is working with Member States and its stakeholders to transpose the recent amendment number 16 of Annex 17[32] (Security) to the Convention on International Civil Aviation adopted by the ICAO Council on 14 March 2018 into EU legislation. This amendment elevated a recommendation on cybersecurity into a standard (Article 4.9.1.), therefore its implementation is binding upon all ICAO Contracting States. Further, in January 2019, the first Cybersecurity conference[33] in transport took place in Lisbon to bring together different actors of the transport sector and to explore cross-modal cooperation.

The specificities of cybersecurity in the energy sector are also being discussed in a number of existing security of supply expert groups, such as the Electricity Coordination group or the Gas Coordination Group, to bridge any potential gaps between more traditional security-of-supply approaches and specific cybersecurity needs. All these actions are complemented and supported by the work of other Commission services, such as the Directorate General Joint Research Centre (DG JRC, the European Commission's science and knowledge management service) and Agencies, such as the European Union Agency for Network and Information Security (ENISA). Annex 2 provides a detailed overview of their recent activities in the field of cybersecurity in the energy sector.

5. INTERNATIONAL STANDARDS

There are numerous concepts and standards for cyber security, risk management and business continuity since decades. ISO[34], the international organisation for standardisation, and IEC[35], the international Electrotechnical Commission, are the main international organisations for worldwide standardisation.

There are different categories (technical, procedural and others) of standards. The existing standards related to cyber security and risk management are not in contradiction to the three particularities of cyber security in the energy sector, identified in chapter 3. On the contrary, it is advisable to develop any cyber security concept for the power grid on the basis of internationally acknowledged standards, and to keep its specificities in mind when doing so.

[32] https://www.icao.int/security/sfp/pages/annex17.aspx
[33] https://www.enisa.europa.eu/events/first-transport-cyber-security-conference
[34] https://www.iso.org/home.html
[35] http://www.iec.ch/standardsdev/publications/is.htm

Among the international standards, in this context, it is worth to mention, but with no means to limit to, the ISO/IEC 27000 series, IEC62443, IEC62351 and ISO/IEC 31000.

The ISO/IEC 27000 family of information security standards provides a globally recognised framework for information security management. Within this series, the ISO/IEC 27001 standard defines the requirements against which an organisation's information security management system (ISMS) can be audited and certified. ISO/IEC 27019 of 2017 builds upon ISO/IEC 27002 and provides guiding principles for information security management applied in process control systems as such used in the energy utility industry.

IEC 62443 is a series of standards on cybersecurity for Industrial Automation and Control Systems (IACS). By using the techniques described within this series, industrial stakeholders can assess the cybersecurity risks to each system and decide how to address those risks. Due to the fact that not every system is equally critical, there are five security levels defined within the IEC 62443: from SL 0 (no security) to SL 4 (resistant against nation-state attacks).

Specific security requirements are defined for each security level so each industrial system will have the right security, protecting uptime, safety, and intellectual property. All parties in the industrial ecosystem benefit from having clear expectations: asset owners and operators, systems integrators, equipment and service providers, and regulators.

IEC 62351 on "Information Security for Power System Control Operations" provides a set of documents describing standards for implementing selected security solution in power systems. The document series is not providing a taxonomy for mitigations but defines how to implement recommended security systems.

The ISO/IEC 31000 suite of standards is related to risk management. The 31000:2018 provides principles, framework and guidance for risk management processes. It is sector-neutral and threat-oriented. Organizations can use it to compare their risk management practices with an internationally recognised benchmark facilitating in this way comparison in a maturity model context.

This section is limited to give a short overview of only a number of international standards related to cybersecurity and risk management and should under no circumstances be seen as exhaustive.

6. CONCLUSIONS

The energy system is one of the most complex and largest infrastructures in Europe and is also one of the most critical assets for a modern society. The electricity grid is as such the backbone for its economic activities, welfare and stability.

When our energy system was established, cybersecurity was not an issue. Today, the energy sector is undergoing a very rapid change. With the clean energy transition, the share of electricity in the energy mix is expected to double in the long term and the large majority of this electricity will come from renewables. This means that the system will have to handle more variable generation and new aspects of decentralisation. This can be managed only with enhanced digitalisation which brings new challenges for the sector, in particular with respect to cyber security.

Due to the technical features of its infrastructure and components, the energy sector has specific challenges in terms of cybersecurity. Thus, it is indispensable to address these particularities effectively when implementing cyber security in the energy sector.

Member States and energy sector stakeholders concerned are thus invited to take into account the Commission's Recommendation on cybersecurity in the energy sector and the background information provided in this accompanying Staff Working Document.

ANNEX 1: RELEVANT EXPERT AND STAKEHOLDERS FORUMS AND ACTIVITIES

1.1. Energy Expert Cybersecurity Platform

In December 2015, DG Energy - in cooperation with other Commission services - set up the Energy Expert Cyber Security Platform (EECSP) composed of selected experts. This dedicated Expert Group, had the mandate to analyse the specific needs of the energy sector in terms of cyber security. The Expert Group delivered its final report in February 2017[36]. The report identifies the strategic challenges and specific needs of the whole energy sector regarding cyber security from four key angles: threat and risk management, cyber defence, cyber resilience and required capacity and competences needed. The report further analysed to what extent existing legislation at EU and national level is sufficient to tackle the specific needs of the energy sector and proposed a roadmap with actions such as the identification of providers of essential services in energy, the definition of the rules for a regional cooperation or the setting up of a the response framework and coordination.

1.2. Smart Grids Task Force – Expert Group 2 and Stakeholder Working group

As a direct action following from the Clean Energy for All Europeans package, the European Commission set up in spring 2017 a Stakeholder Working Group to further develop the work already carried out by the Energy Expert Cyber Security Platform (EECSP)-Expert Group. The new Stakeholder Working Group was composed of representatives of energy operators (TSOs, DSOs), industry, energy regulators and consumers. It focused on practical approaches and solutions to improve the resilience of the energy network. The recommendations to the European Commission of the working group were finalised beginning of 2019.

The work of the Stakeholder Working Group is part of the Smart Grids Task Force, a broader initiative that has the objective to advice on policy and regulatory issues related to smart grid deployment and development. The Task Force was set up in 2009 by the Commission and currently consists of five Expert Groups[37], which work on specific areas. Expert Group 2 aims to mitigate the risks to personal data and security of smart metering systems. In October 2016, Expert Group 2 delivered a report on the Identification and Selection of Best Available Techniques[38] that addresses the risks related to privacy and security.

1.3. Security of Supply Expert Groups

[36] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

[37] https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force

[38] https://ec.europa.eu/energy/sites/ener/files/documents/bat_wp2_techniques_mapping_and_clustering.pdf

The Electricity Coordination Group (ECG) was established by the Commission in in 2012[39]. Its tasks are to serve as a platform for the exchange of information and coordination of electricity policy measures having a cross- border impact and for the exchange of experiences, best practices and expertise and also to assist the Commission in designing its policy initiatives. It should also facilitate the exchange of information and cooperation regarding security of supply in electricity, including generation adequacy and cross-border grid stability.

The members of the ECG are Member States' authorities, in particular Ministries competent for energy, the National Regulatory Authorities for energy, the Agency for the Cooperation of Energy Regulators (ACER) and the European Network of Transmission System Operators for Electricity (ENTSO-E).

The ECG meets regularly and in recent meetings it has addressed cybersecurity concerns in the energy sector as well as risks and opportunities of digitalisation.

As for the gas sector, the Gas Coordination Group (GCG) was created in 2004 to facilitate the coordination of measures concerning security of gas supply. It is composed of representatives of the Member States, the Agency for the Cooperation of Energy Regulators (ACER), the European Network of Transmission System Operators for Gas (ENTSOG) and representative bodies of industry concerned and consumers.

The GCG meets typically four times a year. Cybersecurity in the gas sector has been part of the GCG agenda in recent meetings and it is expected that in the future it will continue to feature in the agenda, notably in the light of the obligations for Member States to specifically include cybersecurity as part of the risks to be included in their national and regional ("common") Risk Assessments for gas.

1.4. Stakeholder hearings

Following up on the work of the EECSP, DG Energy took a deeper look at the specificities of the energy sector between Mid-2017 to December 2018 and identified the three main particularities of the energy sector: cascading effects, real-time requirements as well as the combination of legacy technologies with smart devices.

Early 2018, DG Energy organised a series of stakeholder[40] hearings to further investigate these particularities with all main stakeholders relevant for the energy sector to get a better understanding of the concerns of the energy sector and how stakeholders see the

[39] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32012D1117(01)

[40] Stakeholders consulted include the European Network of Transmission System Operators for Electricity (ENTSO-E), the European Network of Transmission System Operators for Gas (ENTSO-G), the European Cybersecurity Organization (ECSO), The Union of the Electricity Industry (Eurelectric), The European gas association (Eurogas), the European association of electricity distribution system operators (EDSO), the Groupement Européen des entreprises et Organismes de Distribution d'Energie (GEODE) and the Commission Agencies ACER (Agency for the Co-operation of Energy Regulators) and ENISA (the European Network and Information Security Agency)

role of the EU. The particularities of the energy sector that raise challenges in terms of cyber security were confirmed in these hearings.

The Electricity Regulatory Forum (Florence Forum)[41] also acknowledged that real-time requirements, interconnectivity and the mix of technologies are key energy-specific cyber security challenges that require tailored cyber security approaches. In the conclusions of the 33rd Florence Forum, the Forum called for Commission guidance on key issues addressing both short-term recommendations and developing a medium to long-term framework complementing existing regulation and current initiatives.

In parallel, between April 2017 and May 2018, the Conseil de Cooperation Economique (CCE) also took a deeper look at the particularities of the energy sector and provided technical recommendations on EU guidelines for the energy sector. These recommendations differ from other recommendations related to cyber security as they are completely aligned with the three particularities of the energy sector. In October 2018 further stakeholder workshops took place to discuss the particularities of the energy sector.

1.5. Work stream 8 on energy under then NIS Cooperation Group

As recognized in the Cyber Security Package of September 2017, the specificities of different sectors are important when addressing cybersecurity. In that vein, the NIS Cooperation Group, established under Article 11 of the NIS Directive, included in its First biennial Work Programme (2018-2020), adopted in February 2018, a specific task related to sector-specific aspects. In order to fulfil this task, the Group established a work stream (Work Stream 8) dedicated to the energy sector. This is of particular relevance given the fact that the energy sector was identified as the first sector to be discussed by national competent authorities for the NIS Directive. The Cooperation Group Members expressed already their support for this initiative in the hearings held in early 2018.

The first kick-off meeting of Work Stream 8 was held on 18 June 2018. The Member States present expressed a strong interest to exchange information on the approaches to implement the NIS Directive specifically in the energy sector and to ensure an appropriate coordination between the different activities, including the implementation of the new legislation on security of supply, the network codes and the legislation on critical infrastructure.

1.6. Regular Information Sharing at higher level

[41] The Electricity Regulatory Forum (Florence Forum) was set up to discuss the creation of the internal electricity market. It is currently addressing cross-border trade of electricity, in particular the tarification of cross-border electricity exchanges and the management of scarce interconnection capacity. Participants include national regulatory authorities, Member State governments, the European Commission, TSOs, electricity traders, consumers, network users, and power exchanges. Since 1998 the Forum has met once or twice a year.

In order to raise awareness about cyber security and to promote discussions among different stakeholders, the Commission organised an event on cyber security in the energy sector in the course of the Digital Day in Rome in March 2017 on the occasion of the 60th anniversary of the Treaty of Rome. The conclusions[42] of this event underline the importance of respecting the energy sector's specificities, notably cascading effects, real-time requirements and the link between legacy and new technologies. The outcome of this event fed into a dedicated G7 experts meeting on cyber security in the energy sector in Rome in 2017.

The specific cyber security requirements of the energy sector have also been discussed in the Vienna Cyber Security week 2018, to reach out to those stakeholders that are not subject to the NIS Directive.

In October 2018, a high-level conference dedicated to cybersecurity in the energy sector with around 200 participants took place in Brussels. This event was accompanied with dedicated stakeholder workshops to further discuss the particularities of the energy sector.

1.7. Enhanced cooperation with EE-ISAC

The European Energy – Information Sharing Analysis Centre[43] (EE-ISAC) helps utilities to improve the cyber security and resilience of their grid by enabling trust-based data and information sharing. EE-ISAC was created as result of the DENSEK project[44] (Distributed Energy Security Knowledge) launched by DG HOME of the European Commission in 2015. The EE-ISAC provides a platform for members to share information on cyber security and cyber resilience in the energy sector. Members include European utilities, service providers, academia as well as governmental and non-profit organizations.

The Commission aims to strengthen the position of ISACs as one of the formal follow-up actions to the Cybersecurity Package of 2017. Thus DG ENER participated at several plenary meetings of the EE-ISAC to elaborate further on this cooperation and collaboration.

1.8. Critical Infrastructure Protection Points of Contact (CIP POC) Working Group

This working group was created as consequence of adoption of the ECI Directive. It is composed of the CIP Points of Contact, designated by Member States, to follow up the implementation of the ECI Directive and other actions of EPCIP. The group is managed by the Commission. The CIP POC group meets at least twice a year, more often if

---

42 Digital Day, Rome: Conclusions: https://ec.europa.eu/digital-single-market/en/digital-day & https://ec.europa.eu/energy/sites/ener/files/documents/detailed_minutes_rome_24.3_final.pdf

43 http://www.ee-isac.eu/

44 http://www.densek.eu/

necessary. Its activities are also relevant to the work on all aspects of CIP in the energy sector.

1.9. European Reference Network for Critical Infrastructure Protection (ERNCIP)

The European Reference Network for Critical Infrastructure Protection (ERNCIP) aims at providing a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonise test protocols throughout Europe, leading to better protection of critical infrastructures against all types of threats and hazards and to the creation of a single market for security solutions.

ERNCIP fosters the emergence of innovative, qualified, efficient and competitive security solutions, through the networking of European experimental capabilities. This is a direct response to the lack of harmonised EU-wide testing or certification for CIP products and services, which is a barrier to future development and market acceptance of security solutions. The JRC set up the ERNCIP project in 2009, in the context of the European Programme for Critical Infrastructure Protection (EPCIP), and with the agreement of Member States..

ANNEX 2: AREAS OF WORK OF OTHER COMMISSION SERVICES AND AGENCIES IN THE FIELD OF ENERGY

1.1. Activities by DG JRC

The Joint Research Centre[45] conducts experimental and research activities in the cyber-security and data protection of the Energy Sector. This includes cyber-security research on smart-metering systems, energy Generation, transmission and distribution infrastructures, the interactions between the grid and smart-home devices, as well as the analysis of the cybersecurity maturity of new energy architecture paradigms (renewable energy micro-grids, distributed ledgers based approaches etc). To conduct its on-field research activities JRC take advantage of some dedicated laboratories and platforms:

- The Energy Distributed Ledger platform
- The Cyber-Security Open Space Laboratory
- The Energy Smart-Grid interoperability laboratory
- The Experimental Platform for ICT Contingencies (EPIC)

Moreover, JRC run also the Thematic Network on Critical Energy Infrastructure Protection (TNCEIP)[46] – an initiative of DG ENER, run by DG JRC – made up of European owners and operators of energy infrastructure in the electricity, the gas and the oil sectors. It allows energy sector operators to exchange information on threat assessment, risk management and cyber security.

1.2. Activities by European Union Agency for Network and Information Security

The European Union Agency for Network and Information Security (ENISA) supports the EU's initiatives in the field of cyber security through awareness raising activities and technical reports. The Commission proposed an ambitious reform proposal, including a permanent mandate for ENISA in the Cybersecurity Package[47] of 2017. In the energy field, ENISA has published several reports regarding Smart Grids[48], including:

- Smart Grid Security Certification in Europe
- Smart Grid Security: Recommendations for Europe and Member States
- Appropriate security measures for smart grids
- Communication network interdependencies in smart grids

[45] DG Joint Research Centre (JRC) supports EU policies providing independent evidences and advices throughout the whole policy cycle. DG JRC's activities also cover the energy and cyber-security sectors.

[46] https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure

[47] https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en

48 https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids

ENISA has also published several reports related to ICS/SCADA[49], including energy aspects:

- A study on Communication Network Interdependencies in ICS/SCADA[50]
- Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors
- Certification of Cyber Security skills of ICS/SCADA professionals
- Good Practices for an EU ICS Testing Coordination Capability
- Window of exposure… a real problem for SCADA systems?
- Can we learn from SCADA security incidents?

ENISA is a member of the NIS Directive cooperation group and it has an active role at different levels:

- is the active link to the CSIRTs Network
- brings key knowledge and expertise at plenary meetings
- plays a key role in supporting Work Streams

The Cooperation Group published the following reports (available on the Group's webpage[51]):

- Security measures for OES
- Incident notification for OES

ENISA manages the programme of pan-European cybersecurity exercises named CyberEurope. This is a series of EU-level cyber incident and crisis management exercises for both the public and private sectors from the EU and EFTA Member States. The Cyber Europe 2014 exercise included a scenario that revolved around a proposal for an EU regulation related to Member States' importing of energy resources.

2.3 Activities by Europol (in particular the European Cybercrime Centre)

The European Cybercrime Centre (EC3) at Europol supports law enforcement agencies in Member States in any investigation/emergency response to cyber security incidents affecting the energy sector that are of a suspected criminal nature. EC3 provides intelligence notifications/threat assessments on cybercriminal activities affecting the energy sector as well as trend/threat monitoring (via IOCTA[52], dedicated reports if needed, Cyber Bits, etc.).

[49] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada
[50] https://www.enisa.europa.eu/publications/ics-scada-dependencies
[51] https://ec.europa.eu/digital-single-market/en/nis-cooperation-group
[52] https://www.europol.europa.eu/iocta

ANNEX 3: List of Abbreviations

5G	Fifth generation of broadband cellular network technology
ACER	Agency for the Cooperation of Energy Regulators
AES	Advanced Encryption Standard
CCE	Conseil de Cooperation Economique
CERT-EU	Computer emergency response team for the EU institutions, bodies and agencies
CIP	Critical Infrastructure protection
CIP POC	Critical Infrastructure protection points of contact
CSIRT	Computer security incident response team
DoS attack	Denial of Service attack
DENSEK	Distributed Energy Security Knowledge
DG ENER	Directorate-General for Energy
DG HOME	Directorate-General for Migration and Home Affairs
DG JRC	Directorate-General Joint Research Centre
DMS	Distribution Management System
DSO	Distribution system operator
EC3	European Cybercrime Centre at Europol
ECG	Electricity Coordination Group
ECI	European Critical Infrastructures
EECSP	Energy Expert Cybersecurity Platform
EE-ISAC	European Energy Information sharing and Analysis Centre
EMS	Energy Management System
ENISA	European Union Agency for Network and Information Security

ENTSO-E	European Network of Transmission System Operators for Electricity
ENTSOG	European Network of Transmission System Operators for Gas
EPCIP	European Programme for Critical Infrastructure Protection
ERNCIP	European Reference Network for Critical Infrastructure Protection
EU	European Union
G7	Group of 7
GCG	Gas Coordination Group
GMAC	Galois Message Authentication Code
GOOSE	Generic Object Oriented Substation Event
HMAC	Hash-based message authentication code
IACS	Industrial automation and control systems
ICS	Industrial control system
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IOCTA	Internet organised crime threat assessment
IoT	Internet of Things
IPSec	Internet Protocol Security
ISAC	Information Sharing and Analysis Centre
ISMS	Information security management system
ISO	International organisation for standardisation
IT	Information technology
MAC	Message authentication code
ms	Milliseconds
NATO	North Atlantic Treaty Organisation
NIS Directive	Directive on security of Network and information systems
OES	Operators of essential services

OSI	Open Systems Interconnection
OT	Operational technology
PC	Personal computer
SCADA	Supervisory control and data acquisition
SHA	Secure hash algorithm
SL	Security level
SWD	Staff Working Document
TC57	Technical Committee 57
TNCEIP	Thematic Network on Critical Energy Infrastructure Protection
TSO	Transmission system operator
USB	Universal serial bus
VPN	Virtual Private Network