EUROPEAN
COMMISSION

Brussels, 3.4.2019
C(2019) 2400 final

COMMISSION RECOMMENDATION

of 3.4.2019

on cybersecurity in the energy sector

{SWD(2019) 1240 final}

COMMISSION RECOMMENDATION

of 3.4.2019

on cybersecurity in the energy sector

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Whereas:

(1) The European energy sector is undergoing an important change towards a decarbonised economy, while ensuring security of supply and competitiveness. As part of that energy transition and the related decentralisation of power generation from renewable sources, technological progress, sector coupling, and digitalisation are turning Europe's power grid into a "smart grid". At the same time, this also brings new risks as digitalisation increasingly exposes the energy system to cyberattacks and incidents which may jeopardize the security of energy supply.

(2) The adoption of all eight legislative proposals[1] of the ‘Clean Energy for all Europeans’ Package including the Energy Union Governance as stepping stone, allows to create a favourable environment for the digital transformation of the energy sector. It also acknowledges the importance of cybersecurity in the energy sector. In particular, the recast of the Regulation on the Internal Market for Electricity[2] provides for the adoption of technical rules for electricity such as a Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows, on common minimum requirements, planning, monitoring, reporting and crisis management. The Regulation on Electricity Risk Preparedness[3] broadly follows the approach chosen in the Regulation on Security of Gas Supply[4]; stressing the need to properly assess all risks, including those related to cybersecurity, and proposing to adopt measures to prevent and mitigate those identified risks.

(3) When the Commission adopted the EU Cybersecurity Strategy[5] in 2013, it identified strengthening the Union’s cyber-resilience as a priority. One of the key deliverables of the Strategy is the Directive on Security of Network and Information Systems[6] (hereafter, the "NIS Directive"), which was adopted in July 2016. As the first piece of horizontal EU legislation on cybersecurity, the NIS Directive boosts the overall level of cybersecurity in the

[1] 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.

[2] COM/2016/0861,

[3] COM/2016/0862,

[4] Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply, OJ L 280, 28.10.2017, p. 1.

[5] JOIN(2013) 1

[6] 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.

Union through the development of national cybersecurity capabilities, the increase of EU-level cooperation and the introduction of security and incident reporting obligations for companies referred to as ‘operators of essential services’. Incident reporting is mandatory in key sectors, including the energy sector.

(4) When implementing preparedness measures in cybersecurity, the relevant stakeholders, including operators of essential services in energy as identified under the NIS Directive, should take into account the horizontal guidance issued by the NIS Cooperation Group established under Article 11 of the NIS Directive. That Cooperation Group, which is composed of representatives of Member States, the European Agency for Cybersecurity (ENISA) and the Commission, has adopted guidance documents concerning security measures and incident notification. In June 2018, that Group created a dedicated work stream on energy.

(5) The 2017 Joint Communication on Cybersecurity[7] acknowledges the importance of sector specific considerations and requirements at EU level, including in the energy sector. Cybersecurity and possible policy implications have been the subject of a comprehensive discussion process in the Union over the recent years. Consequently, there is rising awareness today that individual economic sectors face specific cybersecurity issues and, therefore, need to develop their own sectoral approaches in the wider context of general cybersecurity strategies.

(6) Information sharing and trust are key elements in cybersecurity. The Commission aims to increase the sharing of information among the relevant stakeholders by organising dedicated events, as for examples, the high-level roundtable on cybersecurity in energy organised in Rome in March 2017 and the high-level conference on cybersecurity in energy organised in Brussels in October 2018. The Commission also wants to enhance the cooperation between relevant stakeholders and specialised entities such as the European Energy Information Sharing and Analysis Centre.

(7) The Regulation on ENISA, the “EU Cybersecurity Agency”, and on Information and Communication Technology cybersecurity certification (“Cybersecurity Act Regulation[8]”) will strengthen the mandate of the EU Agency for Cybersecurity so as to better support Member States in tackling cybersecurity threats and attacks. It also creates a European cybersecurity framework for the certification of products, processes and services that will be valid throughout the Union and is of particular interest for the energy sector.

(8) The Commission has put forward a Recommendation[9] addressing cybersecurity risks in the 5th generation (5G) of network technologies by setting out guidance on appropriate risk analysis and management measures at national level, on developing a coordinated European risk analysis and on establishing a process to develop a common toolbox of best risk management measures. Once rolled out, 5G networks will form the backbone for a wide range of services essential for the functioning of the internal market and operation of vital societal and economic functions such as energy.

(9) This Recommendation should provide non-exhaustive guidance to Member States and relevant stakeholders, in particular network operators and technology suppliers, for achieving a higher level of cybersecurity in view of the specific real-time requirements identified for

[7] JOIN(2017) 450

[8] 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.

[9] C(2019)2335

the energy sector, cascading effects and the combination of legacy and state-of-the-art technologies. This guidance aims at helping stakeholders keep in mind the specific requirements of the energy sector when implementing internationally recognised cybersecurity standards.[10]

(10) The Commission intends to regularly review this Recommendation based on the progress made across the Union in consultation with Member States and relevant stakeholders. The Commission will continue its efforts to strengthen cybersecurity in the energy sector, notably through the NIS Cooperation Group, which ensures strategic cooperation and exchange of information among Member States in cybersecurity.

HAS ADOPTED THIS RECOMMENDATION:

SUBJECT MATTER

(1) This Recommendation sets out the main issues related to cybersecurity in the energy sector, namely real-time requirements, cascading effects and combination of legacy and state-of-the-art technology, and identifies the main actions for implementing relevant cybersecurity preparedness measures in the energy sector.

(2) In applying this Recommendation, Member States should encourage the relevant stakeholders to build up knowledge and skills related to cybersecurity in the energy sector. Where appropriate, Member States should also include these considerations into their national cybersecurity framework, notably through strategies, laws, regulations and other administrative provisions.

REAL-TIME REQUIREMENTS OF ENERGY INFRASTRUCTURE COMPONENTS

(3) Member States should ensure that the relevant stakeholders, notably energy network operators and technology suppliers, and in particular operators of essential services identified under the NIS Directive, implement the relevant cybersecurity preparedness measures related to real-time requirements in the energy sector. Some elements of the energy system need to work under "real time", that is to say reacting to commands within a few milliseconds, which makes it difficult or even impossible to introduce cybersecurity measures due to a lack of time.

(4) In particular, energy network operators should:

(a) apply the most recent security standards for new installations wherever adequate and consider complementary physical security measures where the installed base of old installations cannot be sufficiently protected by cybersecurity mechanisms;

(b) implement international standards on cybersecurity and adequate specific technical standards for secure real-time communication as soon as respective products become commercially available;

(c) consider real-time constraints in the overall security concept for assets, especially in asset classification;

[10] International Standardisation Organisations have published various cybersecurity (ISO/IEC 27000: Information Technologies) and risk management standards (ISO/IEC31000: Implementation of risk management). A specific standard for the energy sector (ISO/IEC 27019: Information security controls for the energy utility industry) was issued as part of the ISO/IEC 27000 series in October 2017.

(d) consider privately owned networks for tele-protection schemes to ensure the quality of service level required for real-time constraints; when using public communication networks, operators should consider ensuring specific bandwidth allocation, latency requirements and communication security measures;

(e) split the overall system into logical zones and within each zone, define time and process constraints in order to enable the application of suitable cybersecurity measures or to consider alternative protection methods.

(5) Where available, energy network operators should also:

(a) choose a secure communication protocol, taking into consideration real-time requirements, for example between an installation and its management systems (Energy Management System – EMS / Distribution Management System - DMS);

(b) introduce an appropriate authentication mechanism for machine-to-machine communication, addressing real-time requirements.

CASCADING EFFECTS

(6) Member States should ensure that the relevant stakeholders, notably energy network operators and technology suppliers, and in particular operators of essential services identified under the NIS Directive, implement the relevant cybersecurity preparedness measures related to cascading effects in the energy sector. Electricity grids and gas pipelines are strongly interconnected across Europe and a cyber-attack creating an outage or disruption in a part of the energy system might trigger far-reaching cascading effects into other parts of that system.

(7) In applying this Recommendation, Member States should evaluate the interdependencies and criticality of power generation and flexible-demand systems, transmission and distribution substations and lines, and the associated impacted stakeholders (including cross-border situations) in case of a successful cyber-attack or cyber incident. Member States should also ensure that energy network operators have a communication framework with all key stakeholders to share early warning signs and cooperate on crisis management. There should be structured communication channels and agreed formats in place in order to share sensitive information with all relevant stakeholders, Computer Security Incident Response Teams, and relevant authorities.

(8) In particular, energy network operators should:

(a) ensure that new devices, including Internet of Things devices, have and will maintain a level of cybersecurity appropriate to a site's criticality;

(b) adequately consider cyber-physical effects when establishing and periodically reviewing business continuity plans;

(c) establish design criteria and an architecture for a resilient grid, which could be achieved by:

- putting in place in-depth defence measures per site, tailored to a site's criticality;
- identifying critical nodes, both in terms of power production capacity and customer impact; Critical functions of a grid should be designed to mitigate risk that can cause cascading effects by considering redundancy, resilience to phase oscillations and protections against cascaded load cut-off;

- collaborating with other relevant operators and with technology suppliers to prevent cascading effects by applying appropriate measures and services;
- designing and building communication and control networks with a view to confining the effects of any physical and logical failures to limited parts of the networks and to ensuring adequate and swift mitigation measures.

LEGACY AND STATE-OF-THE-ART TECHNOLOGY

(9) Member States should ensure that the relevant stakeholders, notably energy network operators and technology suppliers, and in particular operators of essential services identified under the NIS Directive, implement the relevant cybersecurity preparedness measures related to the combination of legacy and state-of-the-art technology in the energy sector. Indeed, two different types of technologies co-exist in today's energy system: an older technology with a lifespan of 30 to 60 years, designed before cybersecurity considerations, and modern equipment, reflecting state-of-the-art digitalisation and smart devices.

(10) In applying this Recommendation, Member States should encourage energy network operators and technology suppliers to follow the relevant internationally accepted standards on cybersecurity wherever possible. Meanwhile, stakeholders and customers should adopt a cybersecurity-oriented approach when connecting devices to the grid.

(11) In particular, technology suppliers should provide tested solutions for security issues in legacy or new technologies free of charge and as soon as a relevant security issue becomes known.

(12) In particular, energy network operators should:

(a) analyse the risks of connecting legacy and Internet of Things concepts and be aware about internal and external interfaces and their vulnerabilities;

(b) take suitable measures against malicious attacks originating from large numbers of maliciously controlled consumer devices or applications;

(c) establish an automated monitoring and analysis capability for security-related events in legacy and Internet of Things environments, such as unsuccessful attempts to log-in, door alarms for cabinet opening or other events.

(d) conduct on a regular basis specific cybersecurity risk analysis on all legacy installations, especially when connecting old and new technologies; since the legacy installations often represent a very large number of assets, risk analysis might be done by asset classes;

(e) update software and hardware of legacy and Internet of Things systems to the most recent version whenever adequate; in so doing, energy network operators should consider complementary measures such as system segregation or adding external security barriers where patching or updating would be adequate but is not possible, for instance unsupported products;

(f) formulate tenders with cybersecurity in mind, that is to say demand information about security features, demand compliance with existing cybersecurity standards, ensure continuous alerting, patching and mitigation proposals if vulnerabilities are discovered, and clarify vendor liability in the event of cyber-attacks or incidents;

(g) collaborate with technology suppliers to replace legacy systems whenever beneficial for security reasons, but take into account critical system functionalities.

MONITORING

(13) Member States should communicate to the Commission, within 12 months after the adoption of this Recommendation, and every two years thereafter, detailed information regarding the state of implementation of this Recommendation through the NIS Cooperation Group.

REVIEW

(14) On the basis of the information submitted by the Member States, the Commission will review the implementation of this Recommendation and assess whether further measures are required as appropriate in consultation with the Member States and the relevant stakeholders.

ADDRESSEES

(15) This Recommendation is addressed to the Member States.

Done at Brussels, 3.4.2019

For the Commission
Miguel Arias Cañete
Member of the Commission

CERTIFIED COPY
For the Secretary-General,

Jordi AYET PUIGARNAU
Director of the Registry
EUROPEAN COMMISSION