European Commission

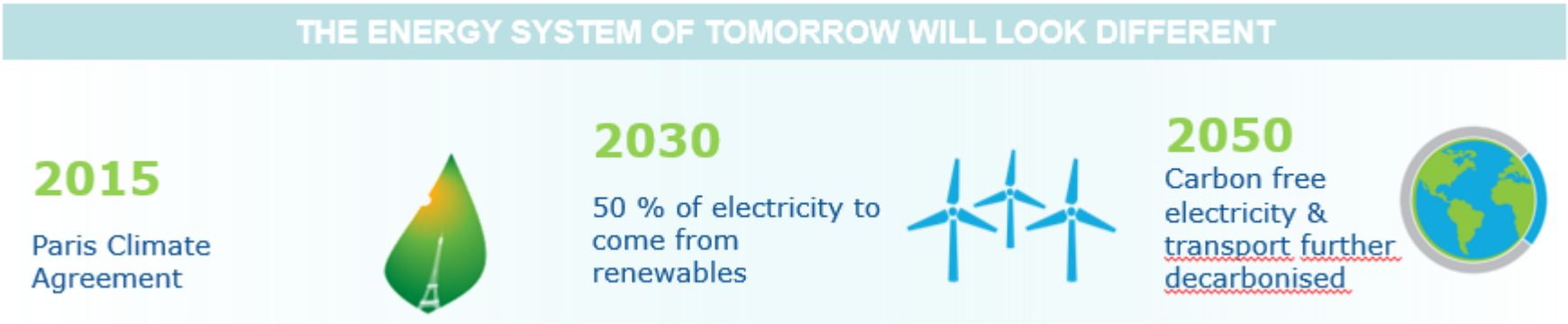
Cybersecurity in the energy sector

11 April 2019

Rémi Mayet
Directorate General for Energy
Deputy Head Security of Supply
European Commission

Energy

The European Energy Sector



- ***Undergoing radical change***
- ***Transition to low carbon economy***
- ***Decentralisation & renewable energy sources***
- ***Digitalisation***
- ***Smart Grids***

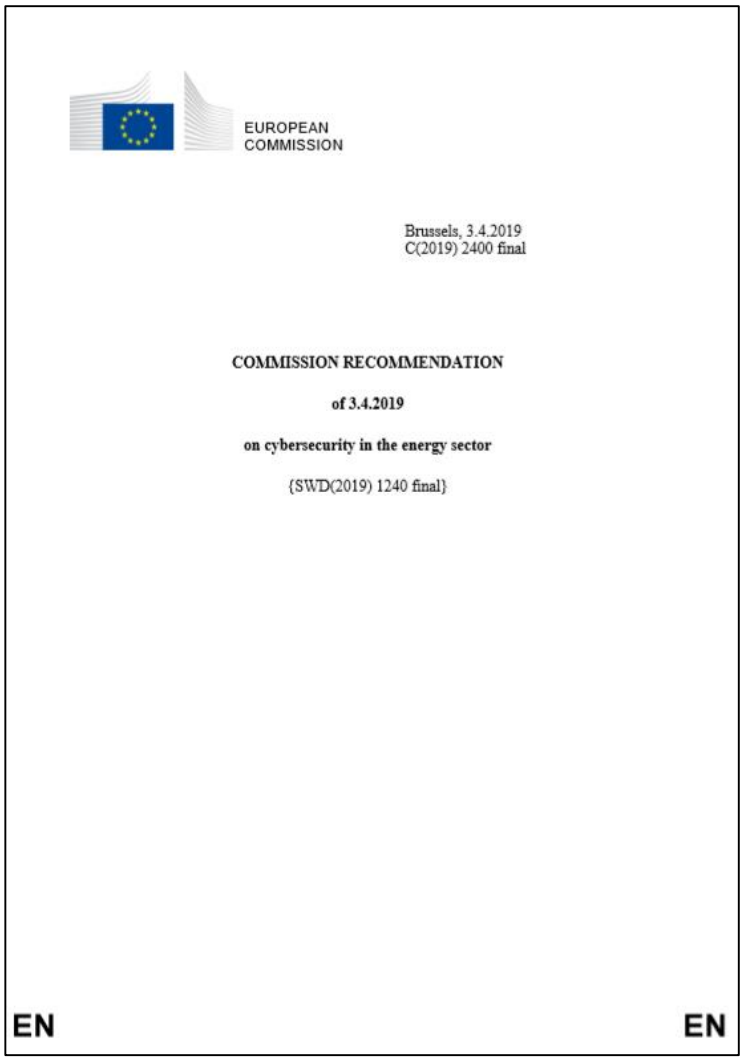
➢ ***Increased risk of cyber-attacks!***

European Commission

European Commission

Commission Recommendation C(2019)2400 final

..on 3 April 2019 the Commission adopted the..



EUROPEAN
COMMISSION

Brussels, 3.4.2019
C(2019) 2400 final

COMMISSION RECOMMENDATION

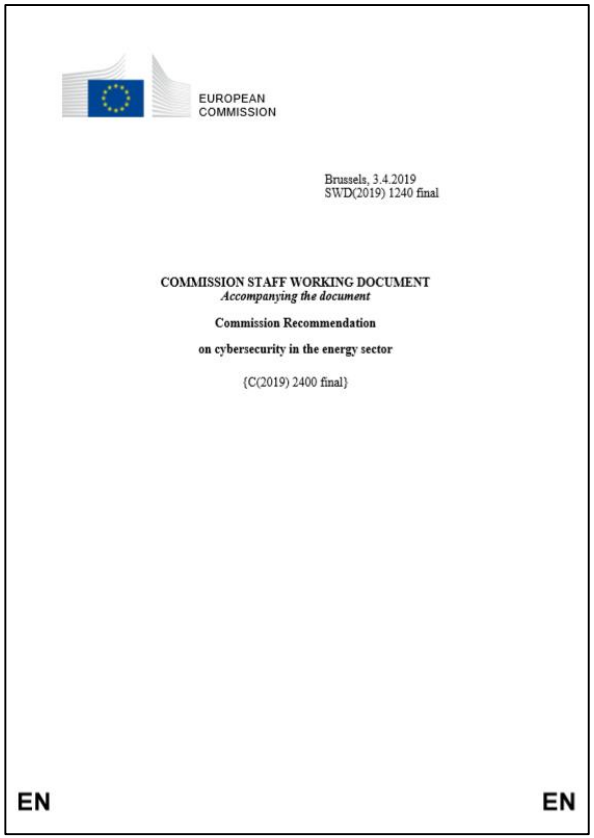
of 3.4.2019

on cybersecurity in the energy sector

{SWD(2019) 1240 final}

EN **EN**

..and the accompanying …



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}

EN **EN**

European Commission

Commission Recommendation C(2019) 2400 final
on cybersecurity in the energy sector

Identifies actions required to address the particularities of the energy sector

Real-time requirements

…simply cannot be addressed by standard cyber security solutions like authentication or encryption.

Cascading effects

…An outage in one country might trigger black-outs in other sectors and countries.

Technology mix

*…creates risks from **legacy** components designed when cyber security was not an issue, and from new **Internet-of-Things** devices not made with cyber security in mind.*

Calls Member States to ensure that the relevant stakeholders take the necessary measures and encourage them to build up knowledge and skills related to cybersecurity in energy

Commission Recommendation C(2019)2400 final

- *Addresses: relevant stakeholders, energy network operators and technology suppliers, and in particular operators of essential services via Member States*

- *Monitoring: within 2 years after adoption, and every two years thereafter through the NIS Cooperation Group.*

- *Review: Assessment of EC in consultation with Member States and relevant stakeholders.*

Recommendations alongside..

Real-time requirements

- *Use international standards*
- *Apply physical measures*
- *Classify/manage your assets*
- *Consider privately owned communication networks, or consider specific measures*
- *Split system into logical zones*
- *Choose secure communication and authentication*

Cascading effects

- *Evaluate interdependencies*
- *Ensure communication framework for early warnings and to cooperate in crisis*
- *Ensure level of security for new devices*
- *Consider cyber-physical spill overs*
- *Establish design criteria for a resilient grid*

Technology mix

- *Follow a cybersecurity-oriented approach when connecting devices*
- *Use international standards*
- *Establish monitoring and analysis capabilities*
- *Conduct specific cybersecurity risk analysis for legacy installations*
- *Collaborate with technology providers*
- *Update hard- and software*

Commission Staff working document SWD(2019) 2400 final

Commission Staff working document SWD(2019) 2400 final

- *Policy context on energy, cybersecurity and critical infrastructure*
- *Technical details of the Recommendation*
- *Inventory of relevant Commission activities*
- *Relevant international standards*

European Commission

Next steps

- *Apply the Recommendation!*
- *Prepare a "Network Code" for electricity*
- *Work on certification of energy technologies*

European Commission

Apply the Recommendation !

Through Regulation (EU) 2017/1938 on Gas Security of Supply and the Regulation on Electricity Risk Preparedness (published May/June)

- **Cybersecurity as part of 1) regional/national Risk Assessments and 2) preventive action and emergency plans**

Through the NIS Cooperation Group

- **Work stream 8 on energy**

Through other outreach activities

- **Dedicated events and networks such as EE-ISAC**

Prepare a "Network Code" for electricity

- *New Electricity Regulation (published in May/June), Art. 59(2)*

  Delegated act on *"Sector-specific rules for cyber security aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management"*

- *Preparatory work on-going*

  Expert Group 2 – Smart Grids Task Force

- *Cooperation with*

  ENTSOE

  Future EU-DSO

  ACER

European Commission

Certification

- *Implement the Cybersecurity Act in energy*

  Identify needs for European Cybersecurity Certificates for energy products, processes and services that will be valid throughout the EU
- *Workshop autumn 2019*
- *Possible input to future Network Code*

Thank you for your attention!!

More information:
https://ec.europa.eu/energy/en/topics/energy-security/critical-infrastructure-and-cybersecurity

Back-up slides

Recommendations alongside..

Real-time requirements

- *Use international standards*
- *Apply physical measures*
- *Classify/manage your assets*
- *Consider privately owned communication networks, or consider specific measures*
- *Split system into logical zones*
- *Choose secure communication and authentication*

Cascading effects

- *Evaluate interdependencies*
- *Ensure communication framework for early warnings and to cooperate in crisis*
- *Ensure level of security for new devices*
- *Consider cyber-physical spill overs*
- *Establish design criteria for a resilient grid*

Technology mix

- *Follow a cybersecurity-oriented approach when connecting devices*
- *Establish monitoring and analysis capabilities*
- *Conduct specific cybersecurity risk analysis for legacy installations*
- *Collaborate with technology providers*
- *Update hard- and software*
- *Formulate tenders with cybersecurity in mind*

Measures related to real-time requirements

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).

- *Apply most **recent security standards & physical measures***
- *Implement **international standards***
- ***Classify your assets** and consider real-time requirements*
- *Consider **privately owned communication networks**; consider specific measures when using public networks*
- *Split the system into **logical zones** and define time and process constraints for each zone*
- *Choose **secure communication protocols** and test prior its implementation*
- *Introduce **appropriate authentication mechanisms** or at least strict network access control mechanisms.*

Measures related to cascading effects

- *Evaluate the **interdependencies** and **criticality of power generation** and **flexible-demand systems**, **transmission** and **distribution** substations and lines, and the **associated impacted stakeholders***
- *Ensure **communication framework** to share **early warning signs** and cooperate on crisis management, incl. structured communication channels and agreed formats for sensitive information*
- *Appropriate **level of security** for new devices, e.g Internet of Thing Devices*
- *Adequately consider **cyber-physical effects***
- *Establishing **design criteria and architecture** for a resilient grid (in-depth defense measures, identifying critical nodes, collaborating with others, design to limit failures)*

Measures related to technology mix

- *Follow a **cybersecurity-oriented approach** when connecting devices to the grid*
- *Follow relevant **international standards***
- ***Provide tested solutions** when security issues become known*
- *Follow relevant **international standards***
- ***Analyse the risks** and take **suitable measures***
- *Establish **automated monitoring** and **analysis** capabilities*
- *Conduct **cybersecurity risk analysis of legacy installations***
- *Collaborate with **technology suppliers** to replace legacy systems*
- ***Update** software and hardware, and consider complementary measures*
- *Formulate **tenders** with cybersecurity in mind*