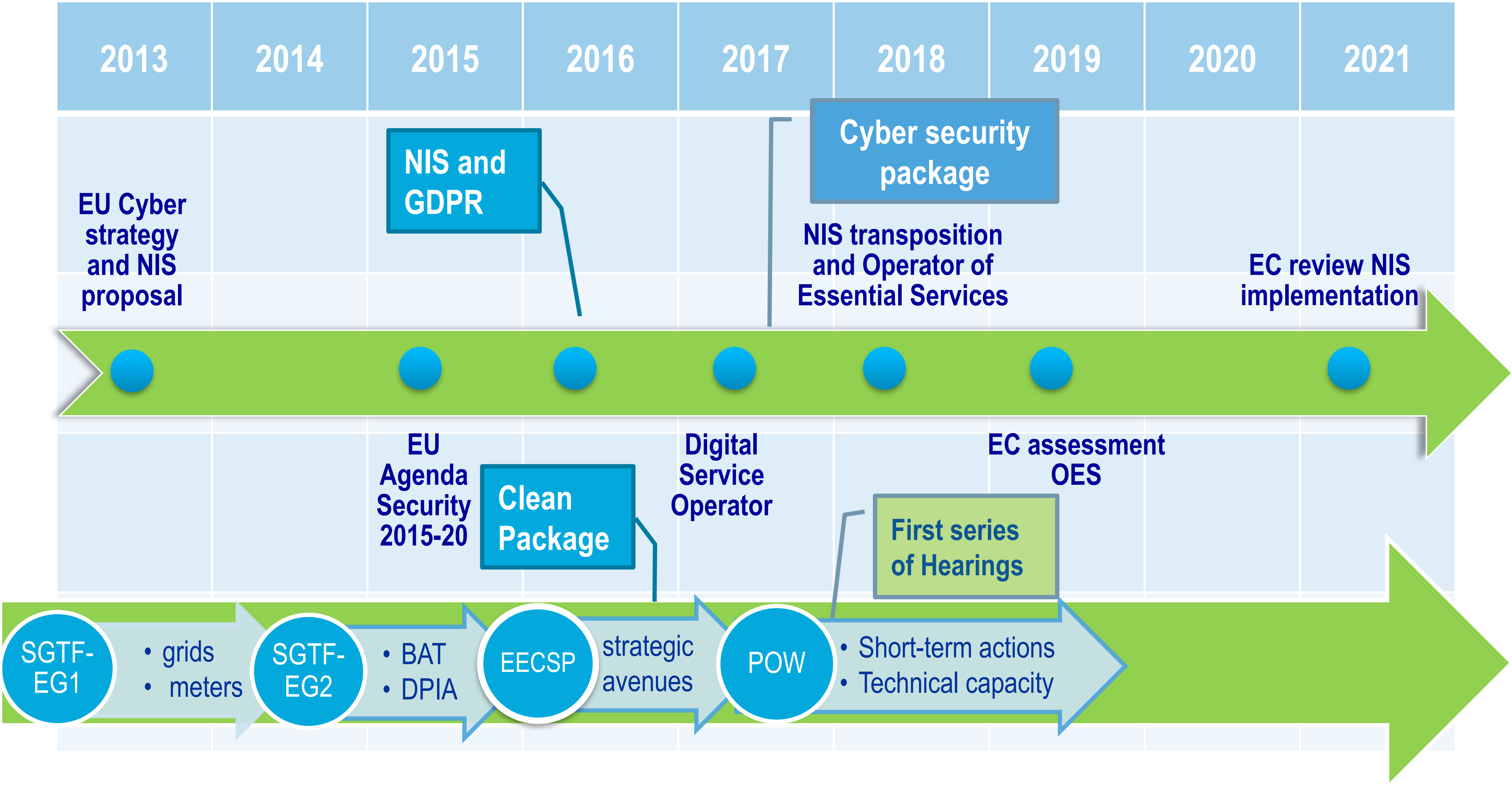
Florence Forum
Session 4.5 - Cybersecurity considerations for the energy sector

Florence 30-31 May 2018

Manuel Sánchez Jiménez
DG ENER - Directorate for Internal Market
European Commission

EU cybersecurity road map and specific energy activities at EU level



2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021

EU Cyber strategy and NIS proposal

NIS and GDPR

Cyber security package

NIS transposition and Operator of Essential Services

EC review NIS implementation

EU Agenda Security 2015-20

Clean Package

Digital Service Operator

EC assessment OES

First series of Hearings

SGTF-EG1
- grids
- meters

SGTF-EG2
- BAT
- DPIA

EECSP
strategic avenues

POW
- Short-term actions
- Technical capacity

European Commission

Key challenges of the energy sector in terms of cyber security

I. Real-time requirements

Some energy systems (e.g. circuit breakers) need to react so fast, that security measures, like authentication of a command, simply cannot be introduced due to the implied delay.

II. Cascading effects

Electricity grids and gas pipelines are strongly interconnected across Europe and well beyond EU Member States. Unlike other IT systems,

i) control systems in the energy sector under attack cannot be easily shut down,

ii) an outage of an energy sector in a region might trigger cascading effects into other sectors or other regions.

III. Legacy systems in combination with new technologies

The energy sector needs to find ways how to embark on a digital future without getting compromised by its analogue legacy

Possible "uncertainties and gaps" identified for the energy sector

I. **Ambitions in national NIS-Strategy may differ among actors, measures, risk assessment and cooperation method for incidents in a (sub)sector**
   - → It might be useful to designate one Competent Authority and Single point of Contact for each sector
   - → It might be useful to clearly define the concrete tasks of CSIRT for energy

II. **NIS is applicable to OESs and DSPs, but not to sectors/subsectors**
   - → open to further (sub)sector's secondary legislation
   - → OESs might not be applied to existing market players, such as balancing responsible, aggregators, metering operators, etc.
   - → DSPs might not be applied to new players, such as aggregator, etc.

III. **Incident Notification:** OES and DSPs have to notify whenever there is a "substantial" or "significant" impact on the provision of a service, but
   - → Each MS have to determine what is a "substantial"/"significant" impact in energy services? What is the preferred format of the information?
   - → Where to draw the line between commercial interest and confidentiality of an operator and the interest to other MS or the public?
   - → When public awareness helps to prevent an incident?

Stakeholder's consultation – main outcome and planned EC actions

Strategic Priorities		Rationale	Short-term actions
I	Guidance on NIS implementation at the energy sector	POW of the NIS Cooperation Group for 2018-20 is open for sector specific aspects, including guidance for NIS implementation	▪ Initiate a subgroup on energy to facilitate NIS implementation.
II	Specific guidance for the energy sector, beyond NIS	There are needs to collectively address, among others: – Minimum technology-neutral cybersecurity requirements for energy infrastructure – Transparency of the supply chain – Ways to secure equipment that cannot be subject to cyber security upgrades	▪ Draft a COM Guidelines or Recommendations based on further stakeholder's consultations ▪ It also might include a Code of Conduct in cooperation with the industry to guarantee good practices
III	Specific events for information sharing at high-level	There is a strong interest into information sharing events about generic cyber issues in the energy sector, such as awareness, cooperation, physical measures, new risks, standards and certification, education, etc.	▪ Events already done and under planning
IV	Support existing European Energy Information Sharing and Analysing Centre	The Cybersecurity Act proposed that ENISA contributes to set up ISACS in various sectors EE-ISAC was already launched in 2015	▪ Set up possible support and appreciation to EE-ISAC

Med-long term actions on technical capacity
Smart Grids Task Force : Expert Group 2

I. **Clean Energy for all Europeans (COM/2016/0860 final)**

II. **Builds up on previous work (e.g. EECSP)**

III. **Set up in spring 2017 and first deliverable by the end of 2018**

IV. **Key areas and subgroups:**

— European Cybersecurity Framework to bring all system operators to a minimum security level with a commitment on continuous improvement.

— Supply Chain Management to create transparency and trust in the use of products, systems and services which are deployed in an electricity grid.

— European Early Warning System for Cyber Threats by sharing security related information like early warning information (indicators of attack/compromise) by utilising existing set-up of CSIRT network.

— Cross-Border and Cross-Organisational Risk Management to define a methodology for a threat and risk analysis and define appropriate mitigation measures.

Questions for the discussion

I. Do you agree with the three specificities of the energy sector with respect to cybersecurity? What additional major specific vulnerabilities?

II. How can energy utilities determine if they are secure? What are the tools to measure and prioritise their investments to improve resilience? What type of incentives are been applied to enhance cybersecurity efforts?

III. What obstacles currently are preventing European public and private agencies from sharing more cyber threat information with energy utilities?

IV. Where would be the emphasis of cybersecurity collaboration to ensure a pan-European improvement? What could be the right level of information exchange and collaboration to start with?

V. Why would or wouldn't EU-wide guidelines for cybersecurity in the energy sector be helpful?

European Commission

Background information

Network and Information Security Directive (NIS)

I. Aim of NIS is:

— to ensure high common level of network and information security,
— improve the security of the internet and private network and information systems,
— increase preparedness of Member States, and
— improve cooperation between Member States

II. NIS defines the following main structure and actions:

— at EU level, create two transnational groups:

✓ MS's Cooperation Group to support and facilitate cooperation and information exchange

✓ Computer Security Incident Response Team (CSIRT) network for operational cooperation and confidence among MSs

— at national level, each MS has to adopt:

✓ National NIS Strategy, including the definition of OESs and DSPs

✓ Set up three existing/additional institutions: National Competent Authority, Single Points of Contacts and CSIRT

✓ Set up national security and notification requirements (for OES and DSP)

Cybersecurity Package (2017)

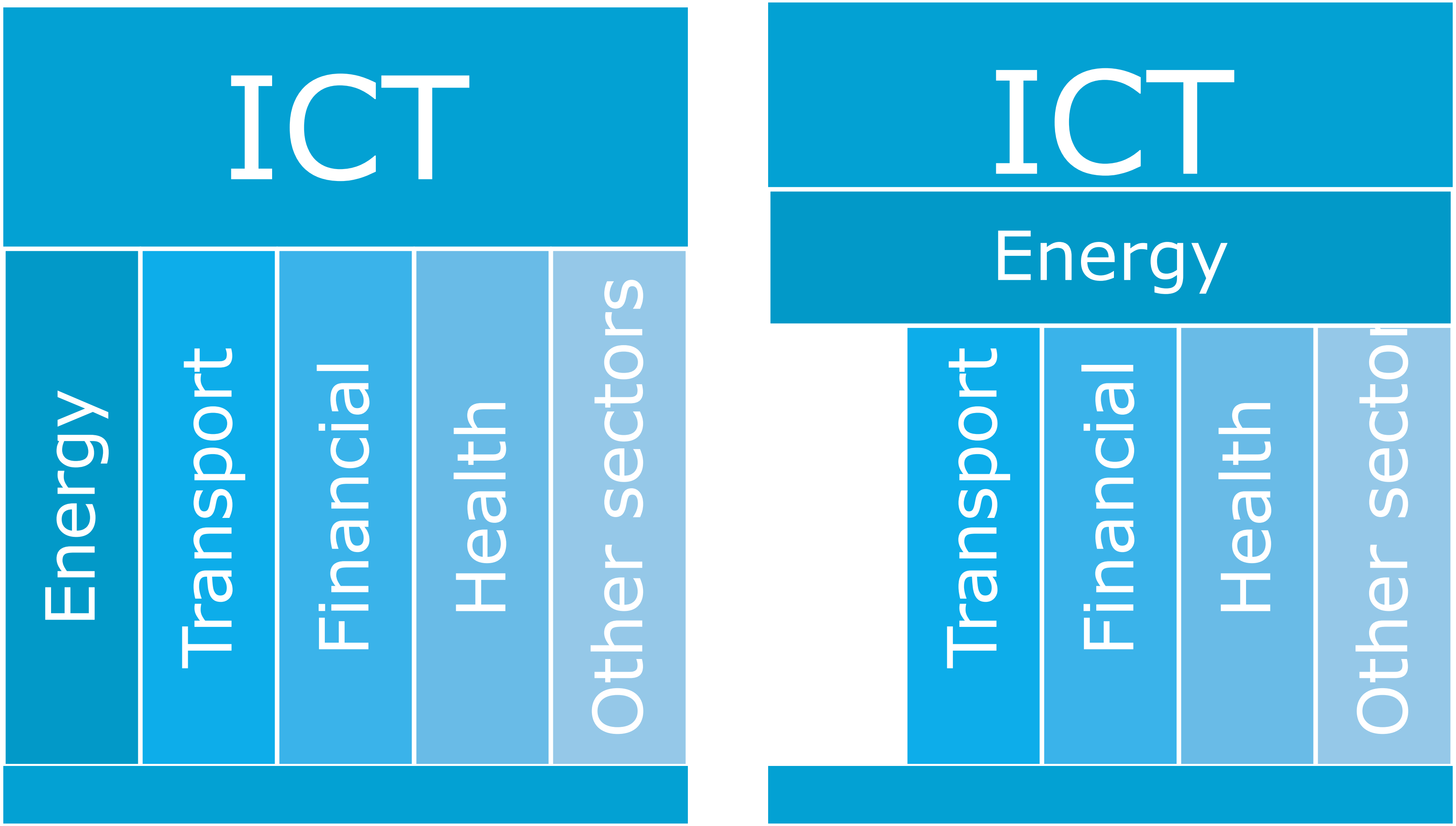
I. EU Cybersecurity Act
- Proposal for a renewal of ENISA's mandate
- Rules for the creation of a European certification framework

II. Blueprint for rapid emergency response

III. Joint Communication on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" – JOIN(2017)450

The Cyber Security Package acknowledges the importance of specificities of different sectors and refers to sector-specific requirements.

What is the role of the energy sector in the cybersecurity strategy?



European Commission