REVISION OF THE NIS DIRECTIVE

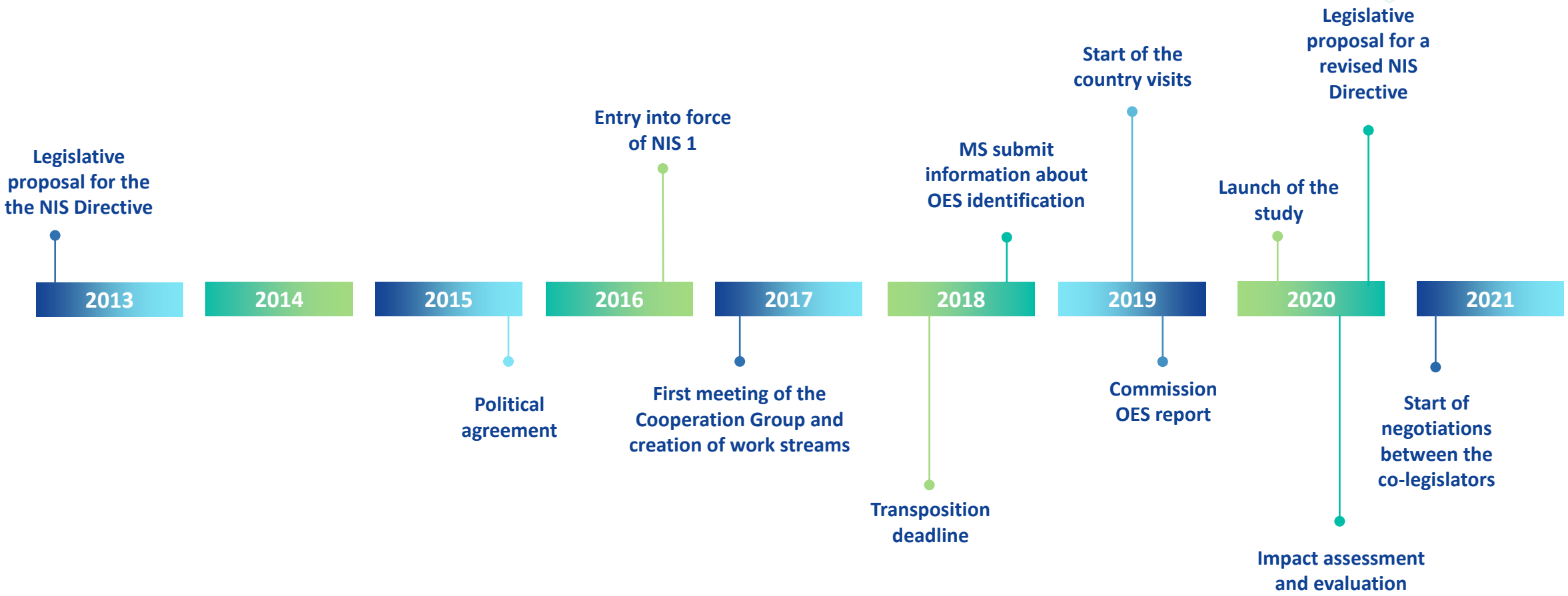
16 March 2021, Cybersecurity in Railways

Svetlana Schuster, Head of Sector, DG CNECT, Unit H2

1 OVERVIEW

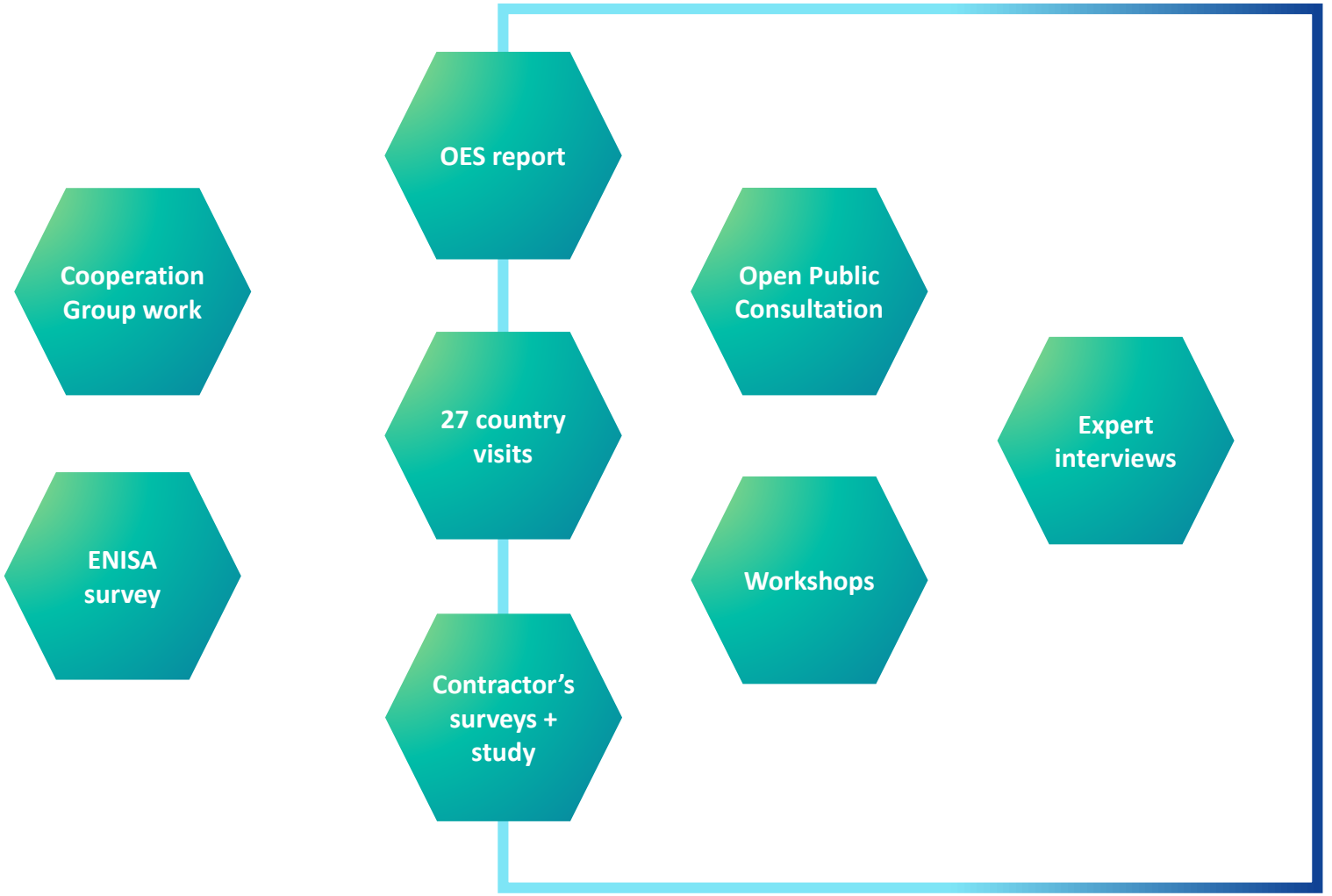
European Commission

Timeline of the NIS Directive



European Commission

Review process throughout 2020



EVALUATION, IMPACT ASSESSMENT + LEGISLATIVE PROPOSAL

European Commission

The NIS 2 vision - main objectives

1

Cover a larger portion of economy and society (**more sectors**)

2

Within sectors: systematically focus on bigger and critical players (**replace current identification process**)

3

Align security requirements (incentivize investments and awareness including by mandating board-level accountability), expand **supply chain** and supplier relationships risk management

4

Streamline incident reporting obligations

5

Align provisions on national supervision and enforcement

6

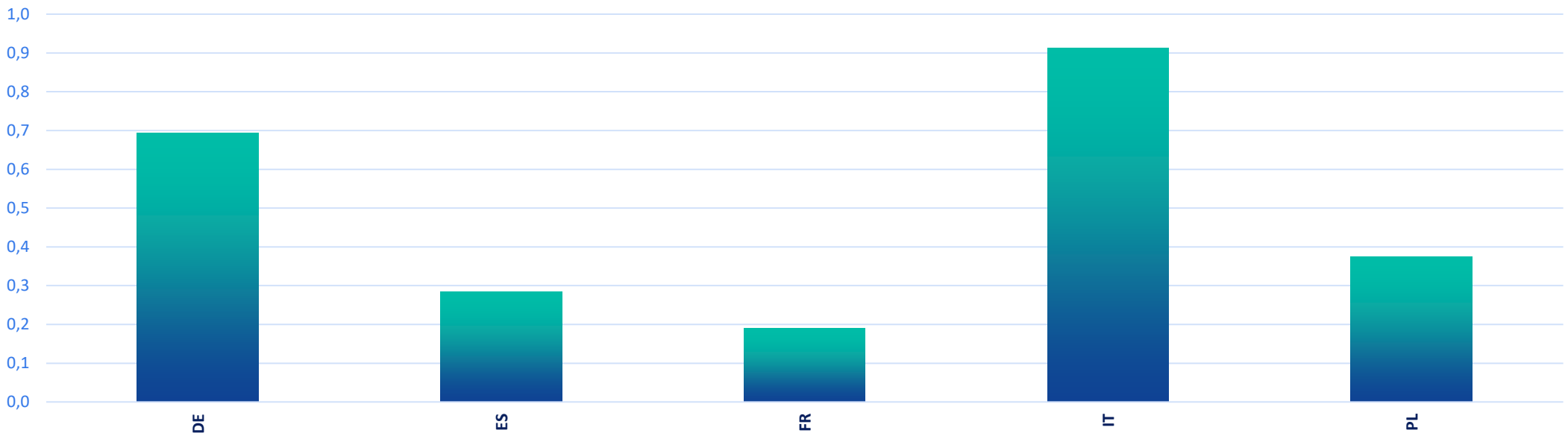
More operational cooperation approach including on crisis management

7

Align with proposed
Resilience of Critical Entities Directive

Main challenges of existing NIS 1

Example: Discrepancies in the identification of operators of essential services (OES)



Identified OES in the five biggest Member States (per 100 000 inhabitants)

European Commission

Three main pillars of the proposal for NIS 2

MEMBER STATE CAPABILITIES

National authorities

National strategies

CVD frameworks

Crisis management frameworks

RISK MANAGEMENT & REPORTING

Accountability for top management for non-compliance

Essential and important companies are required to take security measures

Companies are required to notify significant incidents & cyber threats

COOPERATION AND INFO EXCHANGE

Cooperation Group

CSIRTs network

CyCLONe

CVD and European vulnerability registry

Peer-reviews

Biennial ENISA cybersecurity report

2

MEMBER STATE CAPABILITIES

European Commission

National cybersecurity frameworks

- National cybersecurity strategies
- National **Cybersecurity Crisis Management Frameworks**
- Framework for **Coordinated Vulnerability Disclosure**
- Competent authorities in charge of implementation
- Single Points of Contact (SPOCs) to liaise between Member States
- National Computer Incident Response Teams (CSIRTs)

European Commission

3

RISK MANAGEMENT & REPORTING

European Commission

Which sectors are covered?

Essential entities	Important entities
Energy (electricity*, district heating, oil, gas and hydrogen)	Postal and courier services
Transport (air, rail, water, road)	Waste management
Banking	Chemicals (manufacture, production, distribution)
Financial market infrastructures	Food (production, processing, distribution)
Health (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)	Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)
Drinking water	Digital providers (search engines, online market places and social networks)
Waste water	
Digital Infrastructure (IXP, DNS, TLD, cloud, data centres, CDN, electronic communications and trust service providers)	
Public administrations	
Space	

*** New types of entities in electricity:** electricity markets, production, aggregation, demand response and energy storage

European Commission

Scope based on criticality

SELECTION CRITERIA FOR SECTORS

Existing Member States' policies covering sectors beyond the scope of the NIS Directive

Stakeholders' views reflected from the consultation process

Sectorial **digital intensity**

Level of **importance for society** of sectors, subsectors and services as revealed by a major crisis such as COVID-19

Interdependency among sectors

Scope: size threshold

- **Identification** has proven **inefficient** → difficulty in identifying consistent thresholds
- **Size** as a clear-cut benchmark (all companies, which are medium-sized or larger) and a proxy for importance. **Exceptions:** electronic communications, trust services, TLD registries and public administration.
- **MS** will be in a position to add operators **below the size threshold** in the following cases:
  - **Sole providers** of a service
  - Potential disruption of a service provided by an entity could have an impact on **public safety, public security or public health**
  - Potential disruption of a service provided by an entity could induce **systemic risks**
  - Entities with specific **importance at regional or national level** for a particular sector or type of service, or for other interdependent sectors in a Member State
  - Entities considered as **critical under the proposed Resilience of Critical Entities Directive**

European Commission

Two regulatory regimes

	Essential entities	Important entities
Scope	Scope of NIS1 + certain new sectors	Most new sectors + certain entities from NIS1 scope
Security requirements	Risk-based security obligations, including accountability of top management	
Reporting obligations	Significant incidents and significant cyber-threats	
Supervision	Ex-ante + ex post	Ex-post
Sanctions	Minimum list of administrative sanctions, including fines. Only for essential entities*: ultima ratio* possibility to suspend authorisation or impose temporary ban on managerial duties	
Jurisdiction	General rule: MS where the service is provided Exception: Main establishment + ENISA registry for certain digital infrastructures and digital providers	

More harmonised security requirements

- Accountability for top management for non-compliance with cybersecurity risk management measures
- Risk based approach: appropriate and proportionate technical and organisational measures
- Measures to at least include:
  - risk analysis and information system security policies
  - incident handling
  - business continuity and crisis management
  - supply chain security
  - security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
  - policies and procedures to assess the effectiveness of cybersecurity risk management measures
  - the use of cryptography and encryption

Supply chain security

- Supply chain security is **one of the security measures** that essential and important entities need to take into account
- Member States are required to address cybersecurity in the supply chain for ICT products and services for essential and important entities in their **national cybersecurity strategies**
- The **Cooperation Group** is explicitly empowered with carrying out coordinated security risk assessments of specific critical ICT services, systems or products supply chains (based on the example of 5G)

More harmonised reporting requirements

- Entities to report both significant incidents and cyber threats
- Entities to inform recipients of their services
- Incident notification in **three stages**:

- MS to inform each other and ENISA of incidents with cross-border nature

4

COOPERATION, INFORMATION EXCHANGE AND CRISIS MANAGEMENT

European Commission

Cooperation and information sharing

- **Cooperation Group** gathering competent authorities
- **CSIRTs network** gathering national CSIRTs
- SPOCs to submit **monthly incident summary** reports to ENISA
- Framework of specific **cybersecurity information-sharing arrangements** between companies
- Voluntary information sharing
- **Peer-reviews** of the Member States' effectiveness of cybersecurity policies

European Commission

Coordinated vulnerability disclosure

- As part of the national cybersecurity strategy, Member States will be required to develop a **policy framework on coordinated vulnerability disclosure**
- Each Member State shall be required to designate one **national CSIRT as a coordinator** and facilitator of the coordinated vulnerability disclosure process at national level.
- In cases where the reported vulnerability affects multiple vendors across the Union, the designated CSIRT shall cooperate with the CSIRT network to facilitate multi-vendor coordinated vulnerability disclosure.
- **European vulnerability registry** run by ENISA

European Commission

Crisis management

National Cybersecurity Crisis Management Frameworks

European Cyber Crises Liaison Organisation Network is established to support the coordinated management of large-scale cybersecurity incidents and crises

Thank you for your attention!

European Commission