

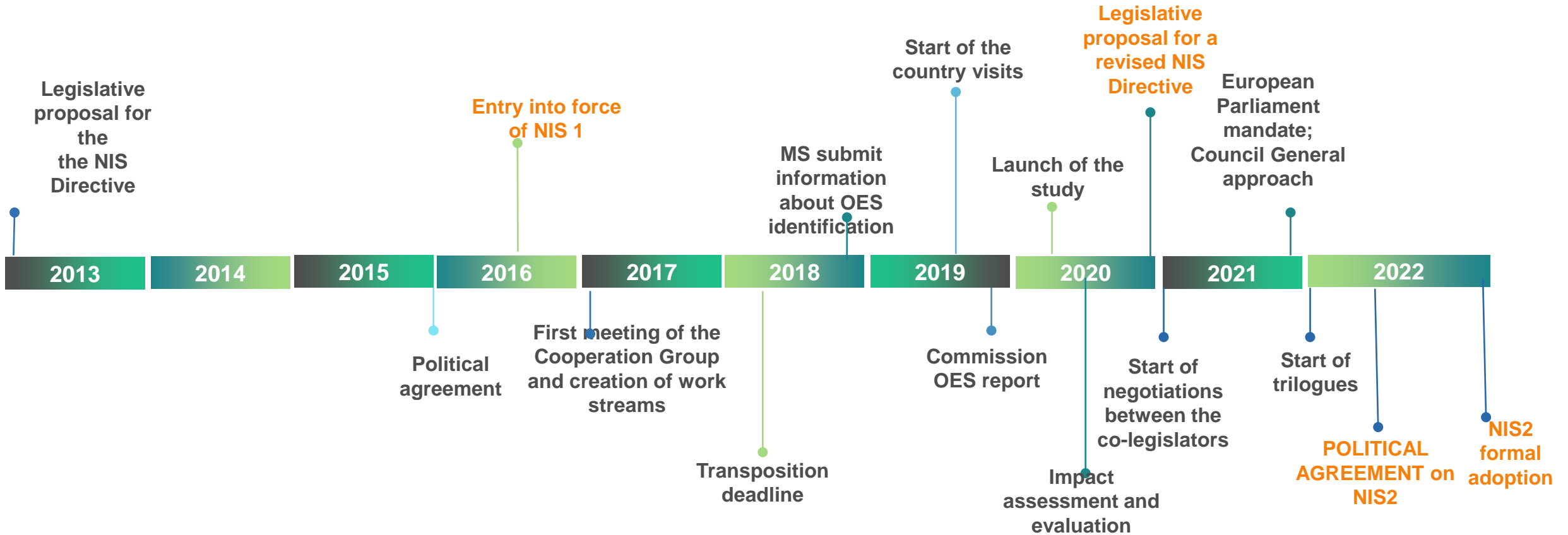


NIS2 implementation and challenges

26 January 2023, EU Cybersecurity Policy Conference, Brussels

*Svetlana Schuster, Head of Sector
Implementation and Review of NIS
Directive, DG CNECT Unit H2*

Timeline of the NIS Directive



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

Three main pillars of the proposal for NIS 2

MEMBER STATE CAPABILITIES



National strategies
National authorities & SPOCs
CSIRTs
CVD frameworks
Crisis management frameworks

RISK MANAGEMENT & REPORTING



Accountability for top management for non-compliance
entities are required to take cybersecurity risk management measures
entities are required to notify significant incidents

COOPERATION AND INFO EXCHANGE



Cooperation Group
CSIRTs network
CyCLONE
CVD and European vulnerability database
Peer-reviews

Which sectors are covered?

Annex I

Energy (electricity (incl. new categories of operators such as electricity producers, nominated market participants, operators of recharging points), district heating and cooling, oil (incl. central stocktaking entities), gas and hydrogen)

Transport (air, rail, water, road)

Banking

Financial market infrastructures

Health (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)

Drinking water

Waste water

Digital Infrastructure (IXP, DNS, TLD, cloud, data centres, Content Delivery Networks, electronic communications, trust service providers,)

ICT Service management

Public administration entities

Space

Annex II

Postal and courier services

Waste management

Chemicals (manufacture, production, distribution)

Food (production, processing, distribution)

Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)

Digital providers (search engines, online market places and social networks)

Research

* New sectors, sub-sectors or type of entities

Two regulatory regimes

	Essential entities	Important entities
Security requirements	Risk-based security obligations, including accountability of top management	
Reporting obligations	Significant incidents	
Supervision	Ex-ante + ex post	Ex-post
Sanctions	Minimum list of administrative sanctions, including fines. Only for essential entities: <i>ultima ratio</i> possibility to suspend authorisation or impose temporary ban on managerial duties	
Jurisdiction	General rule: MS where the entities are established Exception: telcos - MS where they provide services; certain digital infrastructures and digital providers – main establishment in the Union.	

Implementation roadmap: some important implementation tasks or concrete deliverables for Member States, Commission, Cooperation Group, EU-CyCLONe, CSIRTs network and ENISA (1/2)

- ❖ *Member States* have to transpose the NIS2 Directive into national law by 17 October 2024
- ❖ By 17 October 2024, **the Commission** has to adopt implementing acts related to the security and reporting obligations for entities such as the DNS service providers, TLD name registries, cloud computing , managed service providers, managed security service providers, online market place, etc.;
- ❖ By 17 July 2023, **the Commission** has to provide guidelines clarifying the *lex specialis* provision; **the Commission**, with the assistance of ENISA, should also provide, without undue delay, guidelines and templates in relation to the establishment of the list of essential and important entities;
- ❖ By 17 January 2025, the **Cooperation Group**, with the assistance of the Commission and ENISA, and where relevant the CSIRTs network has to establish the methodology and organisational aspects of the peer reviews; **Cooperation Group** should also develop, with the assistance of Commission and ENISA the methodology for self-assessment as well as an appropriate codes of conduct concerning the working methods of cybersecurity experts designated to carry out the peer reviews;

Implementation roadmap: some important implementation tasks/concrete deliverables for Member States, Commission, Cooperation Group, EU-CyCLONe, CSIRTs network and ENISA (2/2)

- ❖ *By 17 January 2025 and every two years thereafter, the **CSIRT network** has to assess the progress made with regard to the operational cooperation and adopt a report;*
- ❖ *By 17 July 2024 and every 18 months thereafter, **EU-CyCLONe** has to submit to the European Parliament and to the Council a report assessing its work;*
- ❖ ***ENISA** is tasked to develop and maintain, after consulting the Cooperation Group, a **European vulnerability database**.*
- ❖ ***ENISA** is tasked also to create and maintain **a registry** of entities providing cross-border services such as DNS service providers, TLD name registries, data centre service providers, cloud computing services and online search engines*
- ❖ ***ENISA** has to adopt, in cooperation with the Commission and the Cooperation Group, **a biennial report** on the state of cybersecurity in the Union.*

Thank you.