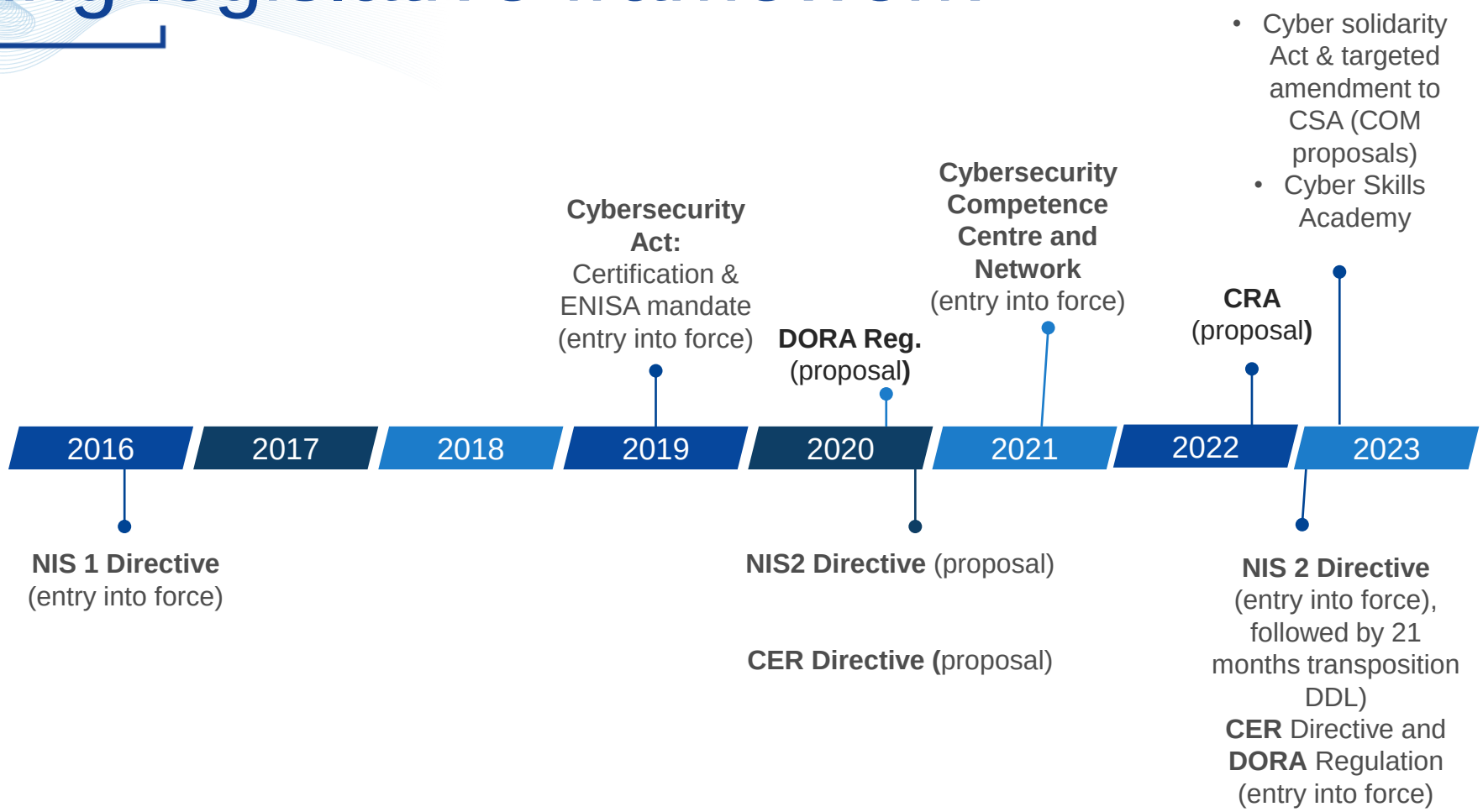
From NIS1.0 to NIS2.0

25 April 2023, NISDUC Conference, Brussels

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

Existing legislative framework



European Commission

Main challenges of NIS 1.0

Not all sectors that may be considered critical are in scope

Great inconsistencies and gaps due to the NIS scope being *de facto* defined by MS (case by case OES identification)

Diverging security requirements across MS

Diverging incident notification requirements

Ineffective supervision and limited enforcement

Voluntary and ad-hoc cooperation and information sharing between MS and between operators

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

European Commission

Which sectors are covered?

Annex I	Annex II
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)	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	Research
Digital Infrastructure (IXP, DNS, TLD, cloud, data centres, Content Delivery Networks, electronic communications, trust service providers,)	
ICT Service management	
Public administration entities	
Space*	

* New sectors, sub-sectors or type of entities

European Commission

Two regulatory regimes

	Essential entities	Important entities
Security requirements	Risk-based security obligations; explicit reference in the law to the applicability of all-hazards approach	
Reporting obligations	Significant incidents	
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 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 concerete 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 securirty and reporting obligations for entities such as the DNS service providers, TLD name registries, cloud computing , managed service providers, managed secuirty 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 organsational 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/concerete 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 regisries, 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.*

European Commission

Thank you.

European Commission