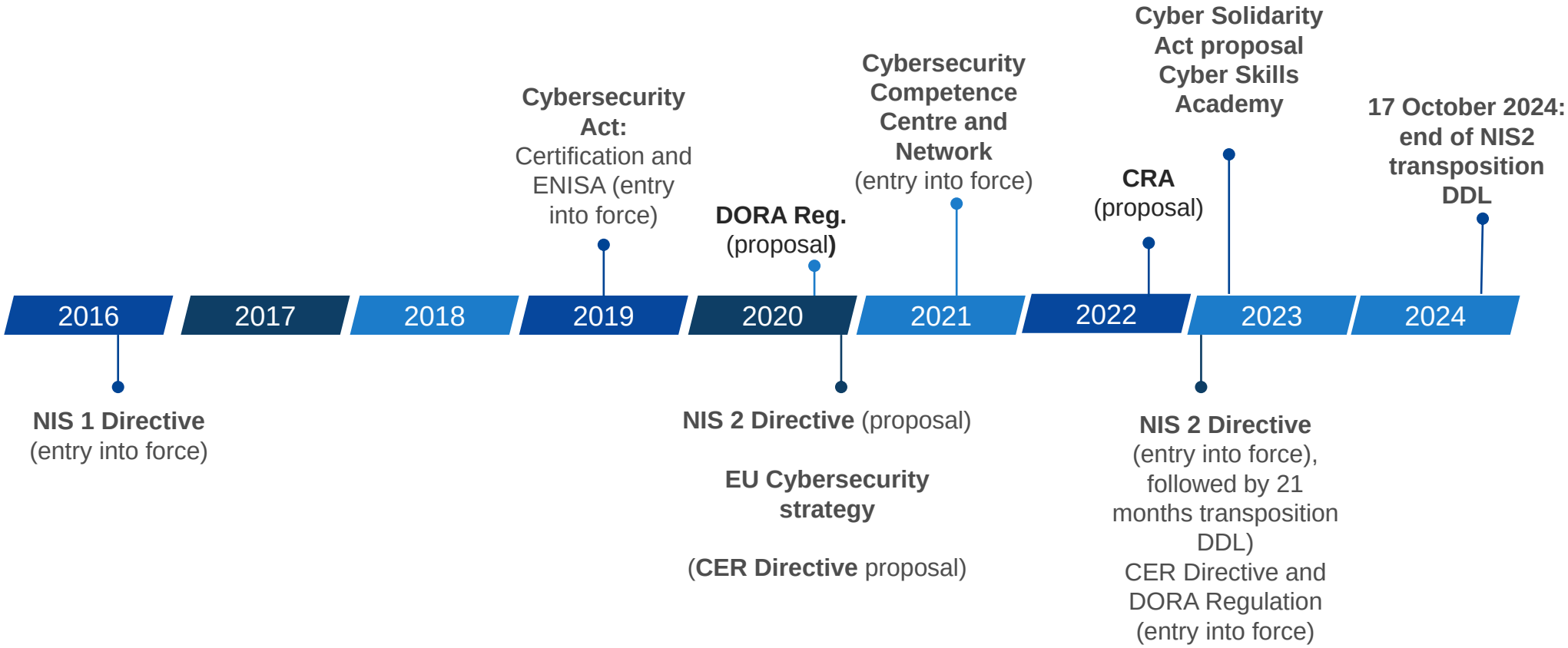
NIS2: brief overview

e-IRG Workshop (22 of June 2023)

Vinzenz Heussler
Unit H2 – Cybersecurity and digital privacy policy
DG CONNECT, European Commission

Existing legislative framework



European Commission

Main challenges of NIS 1 Directive

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 info sharing between MS and between operators

Three main pillars of NIS 2 Directive

MEMBER STATE CAPABILITIES

National authorities

National strategies

Coordinated Vulnerability Disclosure (CVD) frameworks

Crisis management frameworks

RISK MANAGEMENT & REPORTING

Accountability of top management for non-compliance

Streamlined cybersecurity risk management measures for entities, including **supply chain security**

Streamlined incident reporting requirements

COOPERATION AND INFO EXCHANGE

Cooperation Group

CSIRTs network

CyCLONe

CVD and European vulnerability database

Peer-reviews

Biennial ENISA cybersecurity report

European Commission

More harmonised security requirements & incident reporting

- Accountability for top management for non-compliance with cybersecurity risk management measures
- Risk-based approach: appropriate and proportionate cybersecurity measures
- Defining a minimum set of measures

(such as risk analysis and information security policy, incident handling, business continuity, supply chain security)

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

Which sectors are covered by NIS 2?

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	

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.	

Transposition and implementation of NIS 2

- Transposition by the Member States
- Next steps for the Commission

European Commission

Thank you.