



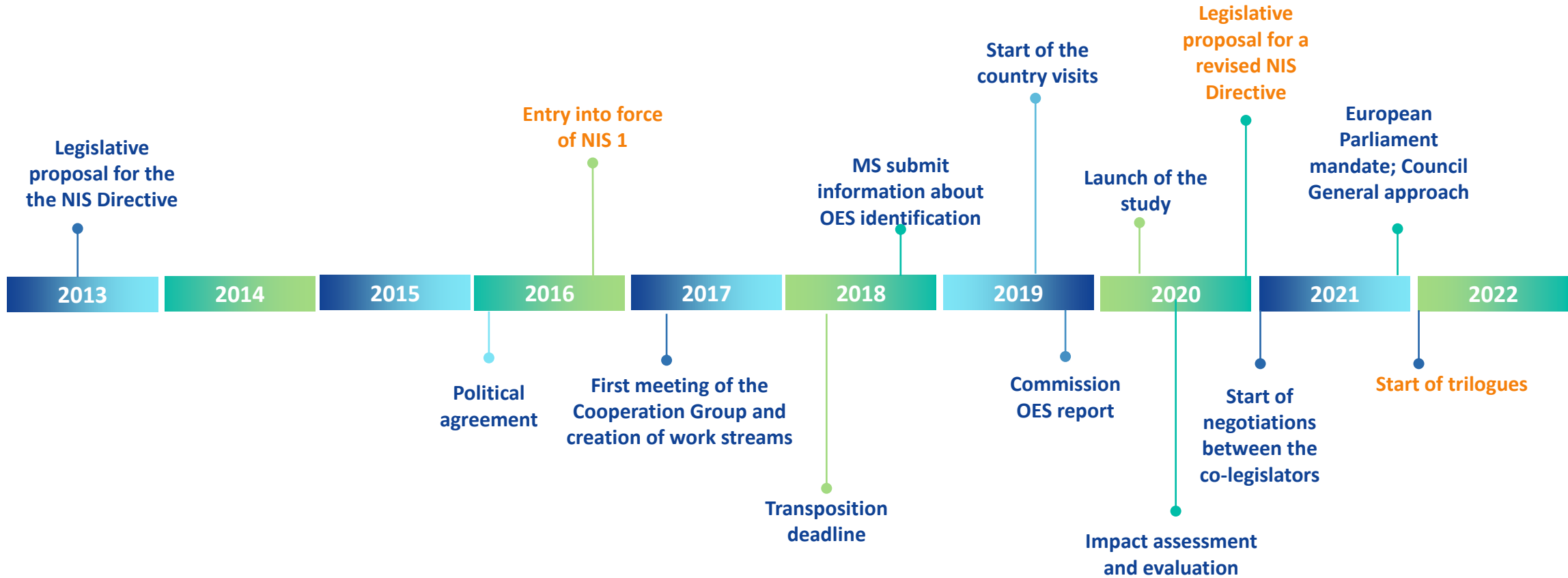
The NIS Directive Revision (NIS 2) State of Play

Boryana HRISTOVA-ILIEVA

Legal officer

*Unit H2 – Cybersecurity and digital privacy
policy DG CNECT, European Commission*

Timeline of the NIS Directive



Main challenges of NIS 1

Not all sectors that may be considered critical are in scope	Great inconsistencies and gaps due to the NIS scope being <i>de facto</i> 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 the proposal for NIS 2

MEMBER STATE CAPABILITIES



National authorities

National strategies

**Coordinated
Vulnerability disclosure
(CVD) frameworks**

**Crisis management
frameworks**

RISK MANAGEMENT



Size threshold

**Accountability for top
management** for non-
compliance

Essential and important
entities are required to
take **security measures**,
including **supply chain
security**

Companies are required
to notify **incidents &
threats**

COOPERATION AND INFO EXCHANGE



Cooperation Group

CSIRTs network

CyCLONE

**CVD and European
vulnerability registry**

Peer-reviews

**Biennial ENISA
cybersecurity report**

**Framework of specific
cybersecurity
information-sharing
arrangements between
companies**

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: <i>ultima ratio</i> 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	

Which sectors are covered?

Main selection criteria: *Existing Member States' policies, stakeholders' views, digital intensity, importance for society (as revealed by COVID-19 crisis), interdependencies between sectors*

Essential entities

Energy (electricity*, district heating, oil, 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, CDN, electronic communications and trust service providers)

Public administrations

Space

Important entities

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)

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

** Infrastructure managers and railway undertakings including operators of service facilities (as defined in Directive 2012/34/EU)

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**



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

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

State of Play of NIS 2 Negotiations

- **European Parliament:** mandate to enter into interinstitutional negotiations adopted on 11 November
- **Council:** the Slovenian Presidency achieved a General Approach, endorsed at the Telecoms Council on 3 December
- **Trilogues:**
 - Already 2 political trilogues under the French Presidency took place (approximately 1 per month), another (potentially last one) planned for 12 May.
 - technical meetings

Thank you!

For contact: boryana.hristova@ec.europa.eu