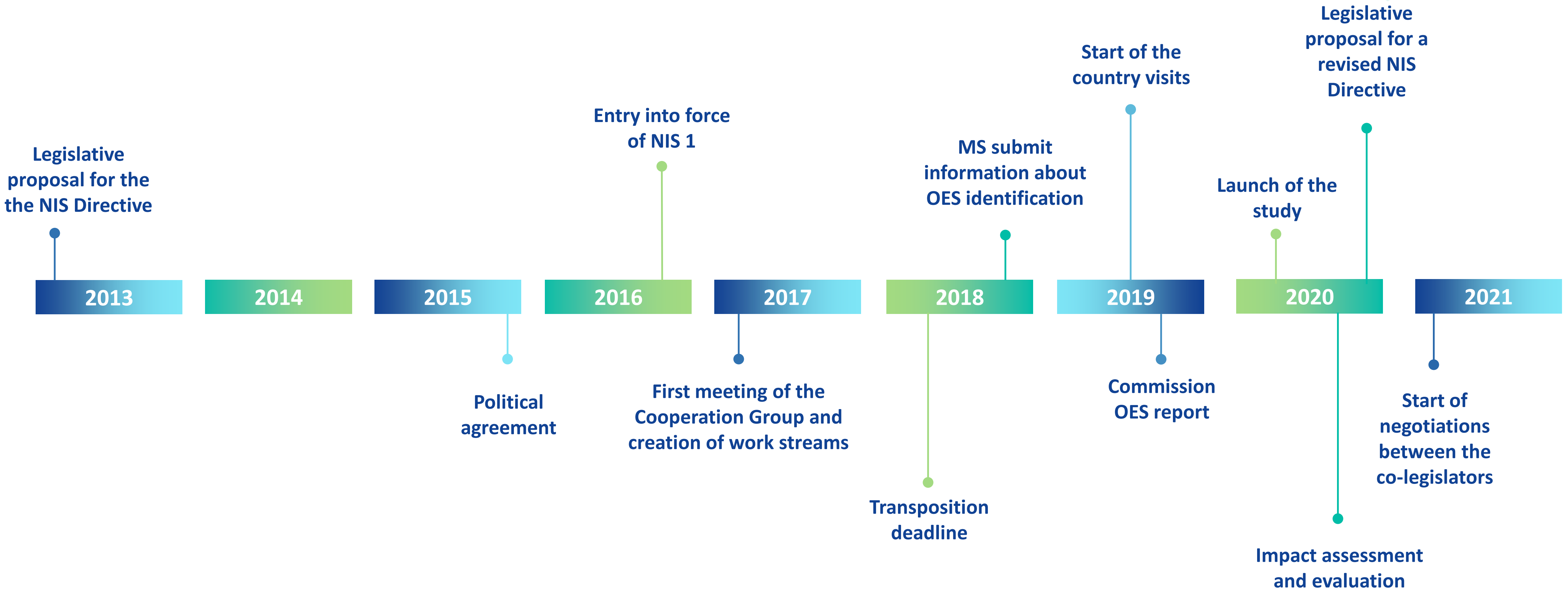
The NIS Directive Revision (NIS 2) State of Play

Boryana HRISTOVA-ILIEVA

Legal officer

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

Timeline of the NIS Directive



2013

Legislative proposal for the the NIS Directive

2014

2015

Political agreement

2016

Entry into force of NIS 1

2017

First meeting of the Cooperation Group and creation of work streams

2018

Transposition deadline

MS submit information about OES identification

2019

Start of the country visits

Commission OES report

2020

Launch of the study

Impact assessment and evaluation

Legislative proposal for a revised NIS Directive

2021

Start of negotiations between the co-legislators

European Commission

Main challenges of existing NIS 1

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

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	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:** producers, NEMOs**,** electricity market participants providing aggregation, demand response or energy storage services

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

European Commission

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

- => **Next step:** interinstitutional negotiations (trilogues) under the French Presidency of the Council

Thank you!

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

European Commission