



An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications



—
NATIONAL
CYBER
SECURITY
CENTRE
—

Proposed New Cybersecurity Directive (NIS 2.0)

NIS 2.0

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

<https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union>

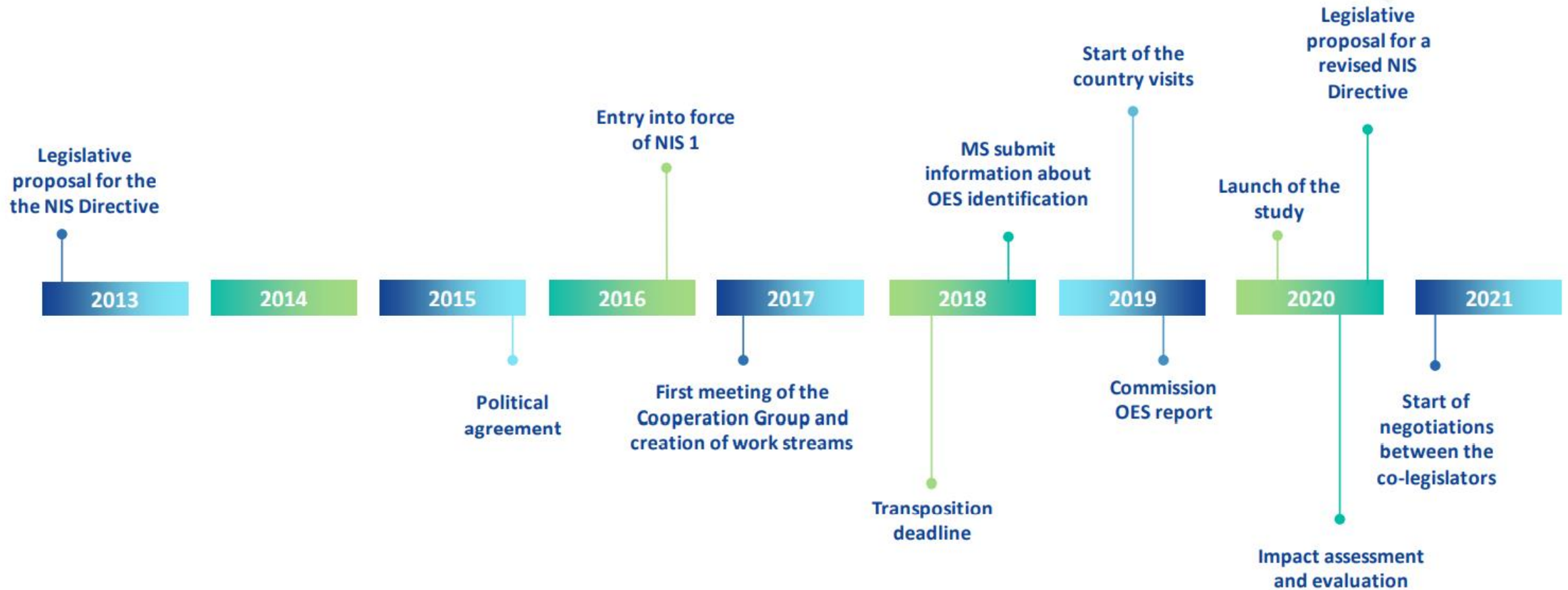


Overview

- European Commission's Review of NIS Directive
- Main Provisions of the new Proposed Directive
- Outlook and Next Steps
- Questions and Answers



Timeline of the NIS Directive



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 info sharing between MS and between operators



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**

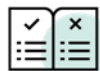
7

Align with proposed **Resilience of Critical Entities Directive**



Three main pillars of the proposal for NIS 2

MEMBER STATE CAPABILITIES



National authorities
National strategies
CVD frameworks
Crisis management frameworks

RISK MANAGEMENT



Accountability for top management for non-compliance
Essential and important companies are required to take security measures
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



National cybersecurity frameworks

- National cybersecurity strategies
- National **Cybersecurity Crisis Management Frameworks**
- Framework for **Coordinated Vulnerability Disclosure**
- Competent authorities in charge of implementation
- Single Points of Contact (SPOCs) to liaise between Member States
- National Computer Incident Response Teams (CSIRTs)



Two regulatory regimes

Essential entities

Important entities

	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	



Selection Criteria for Sectors

- Existing Member States' policies covering sectors beyond scope of NIS Directive
- Stakeholders' views reflected from the consultation process
- Sectorial digital intensity
- Level of importance for society of sectors, subsectors and services as revealed by a major crisis such as COVID-19
- Interdependency among sectors



Which sectors are covered?

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



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.
- **Flexibility** for MS to add operators below the size threshold:
 - **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



Cross border Regulatory Aspects

- MS of main establishment –DNS, TLDs, cloud, data centres, content delivery networks, search, online marketplace, social networks
-  EU Agency for Cybersecurity (ENISA) registry of select entities –DNS, TLDs, cloud, data centres, content delivery networks, search, online marketplace, social networks
- Provision for ‘*mutual assistance*’ between authorities on supervision and enforcement including ‘*joint supervisory actions*’



Supply chain security

- Supply chain security is **one of the security measures** that essential and important entities need to take into account
- Member States are required to address cybersecurity in the supply chain for ICT products and services for essential and important entities in their **national cybersecurity strategies**
- The **Cooperation Group** is explicitly empowered with carrying out coordinated security risk assessments of specific critical ICT services, systems or products supply chains (based on the example of 5G)



Use of European cybersecurity certification schemes

Forward looking provision

Establish legal basis for the use of EU cybersecurity certification schemes

Empowers competent authorities to require the use of certified products and the certification of certain processes.

Provides an empowerment to the Commission for delegated acts to require certification of particular products or processes used by essential entities.



Coordinated vulnerability disclosure

- As part of the national cybersecurity strategy, Member States will be required to develop a **policy framework on coordinated vulnerability disclosure**
- Each Member State shall be required to designate one **national CSIRT as a coordinator** and facilitator of the coordinated vulnerability disclosure process at national level.
- In cases where the reported vulnerability affects multiple vendors across the Union, the designated CSIRT shall cooperate with the CSIRT network to facilitate multi-vendor coordinated vulnerability disclosure.
- **European vulnerability registry** run by ENISA



Cooperation and information sharing

- **Cooperation Group** gathering competent authorities
- **CSIRTs network** gathering national CSIRTs
- SPOCs to submit **monthly incident summary** reports to ENISA
- Framework of specific **cybersecurity information-sharing arrangements** between companies
- Voluntary information sharing
- **Peer-reviews** of the Member States' effectiveness of cybersecurity policies



Report on the state of cybersecurity in the Union

- ENISA to issue, in cooperation with the Commission, a **biennial report** on the state of cybersecurity in the Union:
 - **(a) the development of cybersecurity capabilities** across the Union;
 - **(b) the technical, financial and human resources available** to competent authorities and cybersecurity policies, and the implementation of supervisory measures and enforcement actions in light of the outcomes of the peer reviews;
 - **(c) a cybersecurity index** providing for an aggregated assessment of the maturity level of cybersecurity capabilities.
- Report to include concrete cybersecurity policy recommendations.



Outlook

- Proposed Directive Published in December 2020
- Currently under consideration in EU Council & EU Parliament
 - Progress Report at June 2021 Telecoms Council
 - ITRE Committee of EU Parliament to consider amendments in late Spring, first reading anticipated in Autumn 2021



Your Views ?

- Public Consultation underway to help inform Irish negotiating position in the EU Council
 - The closing date for submissions is **5.30pm Friday 19 March 2021**
 - Submissions should include NIS 2.0 in the subject field and be sent by email to cybersecurityconsultations@decc.gov.ie





Questions and Answers

Consultation

Consultation on the proposed revision to the Directive on Security of Network and Information Systems (NIS Directive)

From [Department of the Environment, Climate and Communications](#)

Published on 12 February 2021

Open for submissions from 12 February 2021

Submissions closed 19 March 2021

Last updated on 23 February 2021

Consultation is open

On 16 December 2020, the European Commission published [proposals to revise and update Directive \(EU\) 2016/1148](#) on security of network and information systems (NIS Directive), which is the first piece of EU-wide legislation on cybersecurity and provides legal measures to boost the overall level of cybersecurity in the EU. While the proposed legislation continues the sectoral approach of its predecessor, it provides for a more comprehensive

Part of

Policy areas

[Communications, Media and Digital](#)

Share



Email

