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

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NIS2 Directive

The new legislation for Cyber Security in Europe

NCSC

Who are we?

- Founded in 2011 – Small staff number based on UCD campus
- Currently part of the Department of Environment, Climate & Communications (DECC), will move to Department of Justice
- Responsible for advising and informing Government and Critical National Infrastructure of current cyber security threats
- Managing and assisting in cyber security incidents across government
- Provide guidance and advice to citizens and businesses
- Government accredited CSIRT as part of CSIRTs network
- National competent authority under EU directive 2016/1148 as the primary point of contact for receiving notification of national incidents
- Feed into the Nation Emergency Coordination Centre during national cyber incidents

NCSC

$whoami

- Member of Operations team of the NCSC since 2022
- Incident Response Manager in Security Operations section
- Previous experience:
  - Incident Response Consultant
  - SOC engineering (SOAR, SIEM development)
  - DevOps
  - Infrastructure engineering (Network, Linux, Windows SysAdmin)
- Reserve Defence Force (Communication & Information Services)

Network & Information Systems

Directive EU 2016/1148

- **What are the origins of NIS?**
- “ In 2013, the Commission released the Cybersecurity Strategy of the EU, which laid out a number of fundamental principles underlying the EU approach to cybersecurity, followed by 5 strategic priorities. The proposal for the NIS Directive is made under the first strategic priority ‘Achieving Cyber resilience’ ”
- 2009 publication by the EU Commission:
- “Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”

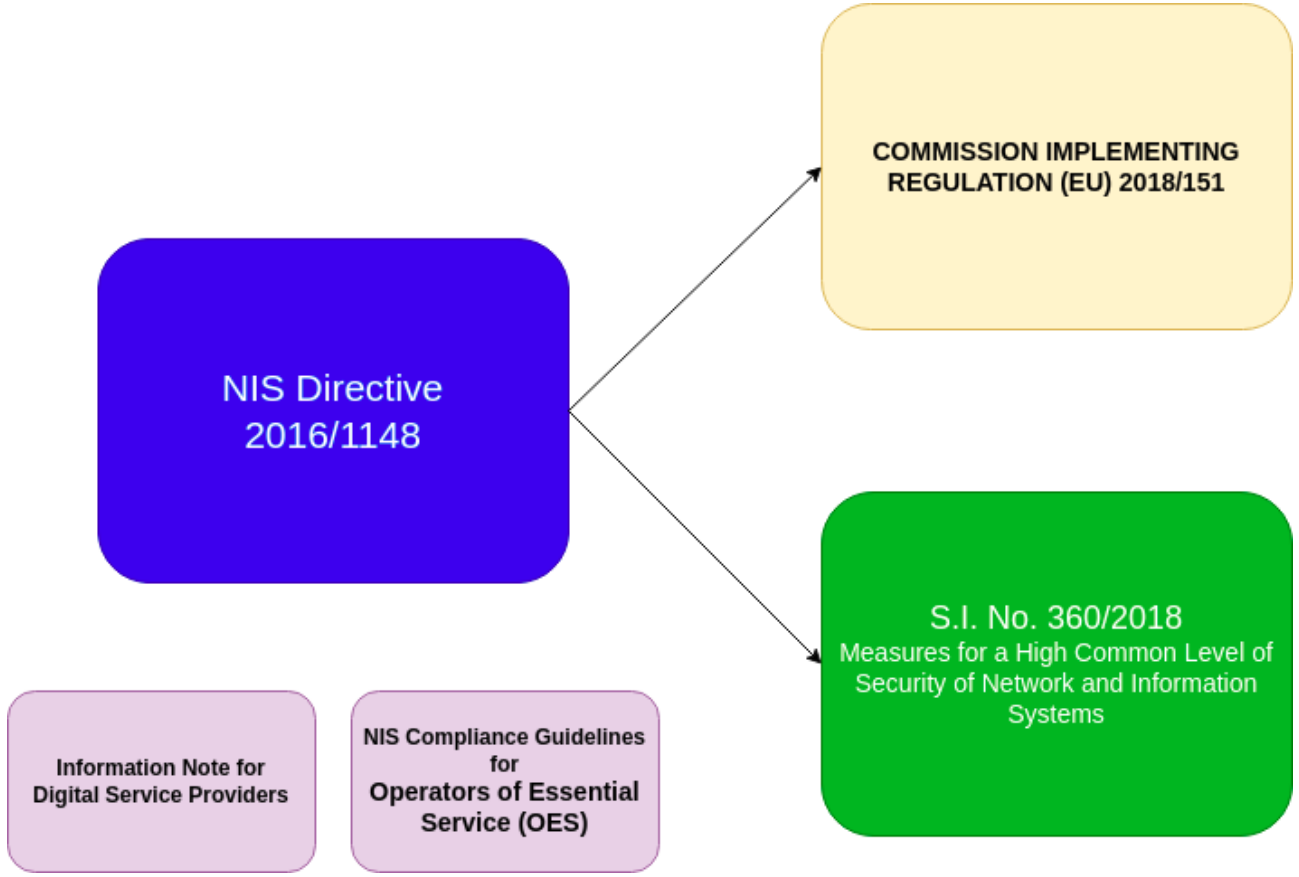
Network & Information Systems

Directive EU 2016/1148

- Improving Cybersecurity: improve the overall level of cybersecurity within the European Union targeting critical services
- Ensuring Security of Essential Services:
  - **Utility** – Water, Energy
  - **Transport** – Shipping, rail, road, air
  - **Finance** - Banking
  - **Health** – Hospitals & other health care providers
- Promoting Cooperation: Establishes a framework for collaboration, ensuring that relevant authorities and entities are working together to prevent and respond to cyber security incidents effectively.
- Risk Management: It promotes a risk-based approach to cyber security, encouraging organizations to assess and manage their cyber security risks.

Network & Information Systems

Directive
EU 2016/1148



Network & Information Systems

Directive EU 2016/1148

- **Designation of National Competent Authorities:**
- Minister for Communications, Climate Action and Environment for all sectors excluding banking and finance
- Central Bank of Ireland – banking and finance

Network & Information Systems

Who is affected?

- **(OES) Operators of Essential Services:**
- Energy: (ESB, Gas Networks Ireland, Bord Gais etc)
- Transport: (Iarnrod Eireann, CIE, DAA)
- Banking: (Central Bank of Ireland, BOI, AIB, KBC, PTSB)
- **(DSP) Digital Service Providers:**
- Cloud service providers: Microsoft, Google, Amazon
- Online market places, Search engines, e-commerce platforms

Network & Information Systems

What are the obligations?

- **Incident reporting**: They must report on incidents of “significant impact” which are sufficient “size”
- **Security measures**: They must implement security measures to ensure the resilience of their networks and information systems.
- **Cooperation**: OES and DSPs are expected to cooperate with the compotent national authorities sharing information and collaborating on matters related to cyber security

Network & Information Systems

Challenges

- First iteration of a common cyber security policy across the EU
- Puts much of the definition onus on EU member states
  - Penalties
  - Security controls
  - OES
- No mention of thresholds for legal terminology
  - Significant impact
  - Size and reach
- None specific and high level. Vague use of language
- Operationally challenging to implement

NIS vs NIS2

Motivation

- **Why create a new NIS Directive?**
- Insufficient level of cyber resilience of businesses operating in the EU
- Inconsistent resilience across Member States and sectors
- Insufficient common understanding of the main threats and challenges among Member States
- Lack of joint crisis response

NIS vs NIS2

Objectives

- **Strengthen security measures:** Enhancing the overall cybersecurity posture of essential entities.
- **Harmonizing obligations:** Establishing uniform incident reporting requirements to improve transparency and enable a coordinated response to cyber threats
- **Expanding the scope of regulation:** Covering a wider range of sectors and digital service providers, reflecting the evolving nature of cyber risks.
- **Cooperation:** Strengthening national supervisory measures and fostering EU-wide collaboration to effectively respond to cyber incidents.

NIS vs NIS2

Scope

- Additional sectors and entities defined
- Clarity on business category thresholds
- **Breakdown into additional categories**
  - Essential (>= 250 employees or €50 million+ revenue)
  - Important (40 – 249 employees or €10 million+ revenue)
  - Not in scope
- **High criticality sectors** (deemed essential)
  - Food production/distrubition
  - Postal services
  - Manufacturing
  - Research
  - Biochemical
- Removal of language such as OES and DSP
  - Replaced by Essential and Important Entities

NIS2

Incident Reporting

24h — EARLY WARNING
Is it a suspected malicious act with potential cross-border impacts?

72h — OFFICIAL INCIDENT NOTIFICATION
Assessment of the incident, severity and impact, plus indicators of compromise.

as requested — INTERMEDIATE STATUS REPORT
At the request of CSIRT or relevant competent authority.

1 month — FINAL REPORT
Or if incident ongoing at time of final report a progress report and final report 1 month after end

NIS2

Enforcement

- Warnings issued for non-compliance
- Binding instructions can be issued
- Cease conduct orders for non-compliance
- Reporting on risk management measures
- Order to inform on cyber threats
- Designated monitoring officer (similar to DPO)
- Order to make public non-compliance
- Cessation of certification for essential entities

NIS2

Penalties

- **Essential Entities:**
  - Maximum of up to €10,000,000
  - Or 2% of total worldwide turnover
- **Important Entities:**
  - Maximum of up to €7,000,000
  - Or 1.4% of total worldwide turnover
- Now on par with GDPR fine structure

NIS2

Risk Management

- **Clearer guidelines on assessment categories**
  - Risk analysis & information system security
  - Incident handling
  - Business continuity measures
  - Supply Chain Security
  - Vulnerability handling and disclosure
  - Policies and procedures on cybersecurity
  - Basic computer hygiene and trainings
  - Policies on appropriate use of cryptography and encryption
  - Human resources security, access control policies and asset management
  - Use of multi-factor, secured voice/video/text comm & secured emergency communication

NIS2 Readiness

What's needed?

Conduct a cyber security risk assessment	Have an incident response plan
Have implemented security controls	Be aware of have established reporting mechanism
Have awareness of the compotent authority	Supply chain security*
Documentation & recording of cyber security strategy	Training & awareness
Legal compliance	Monitoring & auditing

NIS2

Key dates

- December 14th, 2022 – NIS2 Directive published
- January 16th, 2023 – NIS2 adopted by the European Union
- October 17th 2024 - EU member states must include it within their national legislation
- January 17th 2025 – Establishment of of the Cooperation group and CSIRT peer reviews (Delayed)
- April 17th 2025 – Establishment of essential and important entity list within Member states
- October 17th 2027 – NIS2 Directive review

NIS2 & Other Legislation

- **Digital Operational Resilience Act (DORA)** – specific to the Financial sector. More specific measure around ICT protection. Enforced from January 2025. Compotent authority is the Central Bank of Ireland
- **Cyber Resilience Act** – Manufacturing industry. Supply chain focused. Aim addressing specific risk areas. Providers of national digital infrastructure. Cyber Resilience Act applies to radio equipment in scope of the Delegated Regulation adopted under the Radio Equipment Directive 2014/53/EU
- **GDPR** – works in parrellel to NIS2. GDPR safeguards the rights of peoples data. NIS2 works to enhance the security on which this data is stored
- **National Cyber Security Bill** ...

NIS2 & Other Legislation

Publication

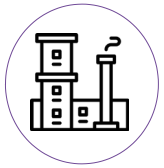
General Scheme of the National Cyber Security Bill 2024

From Department of the Environment, Climate and Communications
Published on 30 August 2024
Last updated on 30 August 2024

On 24 July 2024, the government gave its approval to the priority drafting of the National Cyber Security Bill 2024 in line with the General Scheme published below. The National Cyber Security Bill 2024 is the legislative vehicle for the transposition of the Network and Information Security Directive EU 2022/2555 (NIS2 Directive). It also provides for the establishment of the National Cyber Security Centre (NCSC) on a statutory basis and for related matters including clarity around its mandate and role in general.

We can pass a law to solve that?

Critical Infrastructure



NIS Directive (2016)

First EU-wide cyber directive which aimed to enhance the cybersecurity of critical infrastructure obliging operators of essential services to manage security risks and report significant incidents.

Wider Economy

NIS2 Directive (2022)

NIS2 expands the scope to more sectors, strengthens security requirements, and introduces stricter supervisory measures and enforcement.

Cyber Certification

Cyber Security Act (2019)

Establishes a framework for EU-wide cybersecurity certification schemes for ICT products, services, and processes.

Secure By Design/Default

Cyber Resilience Act (2024)

Mandatory cybersecurity requirements for products with digital elements, aiming to ensure that hardware and software products are designed, developed, and maintained with robust cybersecurity features throughout their lifecycle.

Skills, Research, Industry

ECCC Regulation (2021)

This regulation creates a central EU Cybersecurity Competence Centre to pool resources and expertise, drive research and innovation, and enhance the EU's cybersecurity industrial base and competitiveness.

Monitoring, Detection & Response

Cyber Solidarity Act (2024)

Creating a European Cyber Alert System for detecting and responding to threats, establishing a Cybersecurity Emergency Mechanism with a reserve of incident response companies, and setting up an EU-wide alert system.

Legislation Hierarchy

Overarching Principles

NIS 1 & 2

Sector specific

DORA

CRA

National Implementations

SI 360/2018

NIS2 Summary

- NIS 1 replaced NIS 2 in December 2023
- National transposition on October 17th 2024 (Missed)
- Aims at building on work done by NIS in terms of enhancing national cyber security measures
- Clarifies areas of ambiguity around business thresholds
- Removes the language around OES and DSP, replaced by Essential and important identities
- Introduces larger fines and stricter regulatory penalties in line with GDPR
- Aims to further enhance the cyber resilience of the EU

Contact Us

National Cyber Security Centre, Department of the Environment, Climate and Communications, Tom Johnson House, Beggars Bush, Dublin 4, D04 A068

E emailaddress@ncsc.gov.ie

T +353 (0)1 678 2333

ncsc.gov.ie

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

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre