Directive – 2022/2555
Information Note from the Department
1. Directive Title

Directive (EU) 2022/2555 of the European Parliament and of the Council on 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
2. Transposition Deadline

17/10/2024
3. Anticipated Transposition date

17/10/2024
4. COM number of original Commission proposal

COM/2020/823
5. Department with primary responsibility

Department of Environment, Climate and Communications
6. Other Departments involved

7. Background to, short summary and aim of the directive

The EU cybersecurity rules introduced in 2016 under Directive (EU) 2018/1972, also known as NIS have been updated by Directive (EU) 2022/2555, known as NIS2 came into force in 2023. It modernised the existing legal framework to keep up with increased digitisation and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.
The Directive on measures for a high common level of cybersecurity across the Union (the NIS2 Directive) provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:
• Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national network and information systems (NIS) authority,
• cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States.
• a culture of security across sectors that are vital for our economy and society and that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

Businesses and organisations identified by the Member States as Essential and Important Entities in the above sectors will have to take appropriate security measures and notify relevant national authorities of serious incidents. Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the Directive.
The Directive modernises the existing legal framework taking account of the increased digitisation of the internal market in recent years and an evolving cybersecurity threat landscape. Both developments have been further amplified since the onset of the COVID-19 crisis. The proposal also addresses several weaknesses that prevented the NIS Directive from unlocking its full potential.

The Directive includes increased reporting requirements in terms of what must be reported, to whom must reports be made, and within what timeframe. A much greater range of incidents will need to be reported, since any significant incident has to be notified as will any significant cyber threat that could have potentially resulted in a significant incident. As part of increased supervision and enforcement measures, EU Member States would be required to provide for administrative fines up to at least €10,000,000 or 2% of the total worldwide turnover (at an undertaking level), whichever is higher. Cyber crisis management will also come within the remit of the Directive, and there are also provisions on coordinated vulnerability disclosure and structured information sharing arrangements, and a focus on increased scrutiny of Member State resourcing through peer reviews of Member States' capabilities and resourcing, and obligatory provisions on mutual assistance' between authorities and an EU biennial report on capabilities.
The Directive also includes regulation of top-level domain registries, and their registrars as regards record keeping, transparency and lawful access in accordance with the GDPR. This is to facilitate law enforcement access in the interests of addressing cybercrime.

8. Legal basis of the Directive

Article 114 TFEU

9. Category of Directive

Major significance.

10. Implications for Ireland (including details of regulatory impact assessments carried out in Ireland, if required)

The proposal will build upon and expand the measures introduced by the original Network & Information System Directive to further improve resilience of ICT systems and networks. These provisions were transposed into Irish legislation in S.I. No. 360/2018 - European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018.
A Regulatory Impact Assessment will be completed to accompany this legislation.

11. Impact on the public

The Directive will result in improved services to the public arising from more resilient and more secure ICT systems and networks with increased trust in, reliance on and take-up of digital services.

12. Estimated cost to the Exchequer

No direct costs to the Exchequer expected.

13. Consequences and possible costs, arising from non-transposition

The consequences of non-transposition impact Ireland's ability to operate effectively in a space of increased digitisation and an evolving cybersecurity threat landscape. Recognising the important digital infrastructure and services falling within the scope of the Directive, non-transposition would also have consequences for foreign direct investment and trade policy.
Also according to the EU treaties, the Commission may take legal action – an infringement procedure – against an EU country that fails to implement EU law. The Commission may refer the issue to the Court of Justice, which can impose financial sanctions.

14. Have consultations taken place with stakeholders or are there any plans to do so?

The Department has consulted with and continues to consult with relevant stakeholders including the National Cyber Security Centre, Central Bank of Ireland and other Departments and bodies regarding a range of issues including the designation of competent authorities under the Directive.

15. Are there areas of the Directive where Member States have discretion on implementation?

As this is a Directive Ireland has limited discretion regarding implementation. The Department is currently reviewing the provisions of the Directive in this regard.

16. Does Ireland intend to seek any derogations from the provisions of the Directive?

Not at this time.

17. Offences or penalties (if any) to be created by the transposition of the Directive

The Directive sets out general provisions for supervision and enforcement, imposing administrative fines on essential and important entities and penalties. The Department is currently reviewing the provisions of the Directive in this regard.

18. Competent authorities or market surveillance authorities (if any) to be designated by the transposition of the Directive

Currently two competent authorities are designated under SI 360 of 2018, which transposed Directive (EU) 2016/1148, also known as NIS into Irish law. NIS2 represents a significant broadening and deepening of the regulatory framework established under NIS. The Department is currently reviewing the provisions of the Directive in this regard.

19. Consequences for national legislation?

This Directive will be transposed by primary legislation. The expectation is to bring a Bill through the Houses of the Oireachtas in 2024. Secondary legislation may also be required for the effective implementation of the Directive, in the form of Ministerial Regulations.

20. Are there any parts of the Directive which are planned to be transposed by primary legislation, and if so, which parts?

This Directive will be transposed by Primary legislation.

21. When is it anticipated that the draft statutory instrument(s) transposing this Directive will be available?

This Directive will be transposed by primary legislation.

22. Contact name, telephone number and e-mail address of official in Department with primary responsibility

Cyber Security and Internet Policy Division

Date 11/09/2023