Cyber Security Bill 2024

October 2024 | Pre-Legislative Scrutiny

Input to the Joint Oireachtas Committee on Transport and Communications

Contents

Introduction 2
General Recommendations 3
Recommendations on security and incident reporting obligations 4
Recommendations on supervision, enforcement and penalties 6
Recommendation on the National Cyber Security Centre 8
Other comments 9

Introduction

Ibec welcomes the recent publication of the General Scheme of the National Cyber Security Bill 2024 ('the Bill'), an important step in the transposition of the EU Network and Information Security Directive 2 ('NIS2') in Ireland. Cyber security is an economic and social imperative for Ireland and the EU. In our increasingly digitalised economy and society, it is also key to safeguarding trust in digital tools and protecting our people, businesses, services and critical infrastructure. Government has set a vision for Ireland to be a leading nation in harnessing cyber as an engine of economic growth and societal development.[1] The revised NIS2 Directive, which aims to raise and harmonise the level of cyber security and resilience across the EU, is a central part of this ambition.

We welcome the opportunity to provide comments and recommendations on the Bill.

[1] Department of the Environment, Climate and Communications (2024) Consultation on a Cyber Industrial Strategy

General Recommendations

1. Apply a one-year grace/transition period to allow organisations to bring operations, policies and procedures in line with the requirements of NIS2.

With NIS2 still awaiting transposition in Ireland ahead of the upcoming application date of 18 October 2024, and with uncertainty around aspects of its implementation, a transition/grace period of one year from the date the Bill is signed into law is necessary to allow organisations to review their cyber security posture, prepare compliance plans and provide appropriate updated training to employees.

2. Ensure timely and effective transposition of NIS2 to provide regulatory certainty for entities in scope.

Ireland will play an important role under NIS2, supervising many global entities in the digital infrastructure and digital provider sectors on a pan-European basis. Ireland's standing as an international digital regulatory hub[2] depends on our continued ability to demonstrate leadership in this area, which matters because leadership in digital policy and regulation acts as an investment attractor.[3] Ireland's growing cyber security industry, combining multinational foreign direct investment[4] and a strong indigenous cyber community,[5] also stands to benefit from increased state capacity in this area. Demonstrating leadership through timely and effective transposition of NIS2 should therefore be a priority for Ireland.

In its current form, the Bill also omits key details of NIS2 that should be provided for in the transposing law, particularly details of incident notification requirements e.g. thresholds for identifying 'significant' incidents,[6] templates for incident reports, and practical reporting information.[7] Entities must be notified of the detail of these obligations with sufficient time so that they can be incorporated into compliance plans.

---

[2] Department of an Taoiseach (2021) Harnessing Digital - The Digital Ireland Framework

[3] William Fry and Amarach (2021) Ireland is a Leading Location for Data-Related Investment in the EU

[4] Cyber Ireland 2022, State of the Cyber Security Sector in Ireland and Cyber Ireland 2024, Ireland Cyber Security Sector Snapshot.

[5] Almost half of all cyber security firms operating in Ireland are indigenous. Ibid 2022 and 2024.

[6] **Note**: The definition of a significant incident at Head 15(5) refers to "considerable material or non-material damage." Data protection legislation has referred to "non-material damage" in the context of payment of damages (Article 82 of GDPR), which has proven complicated to determine. The addition of "considerable" under NIS2 adds an additional layer of complexity and potential confusion.

[7] **Note**: Entities in the digital infrastructure, digital provider and ICT service management sectors will be subject to EU measures that will be published the European Commission by 17 October 2024 – see consultation and Ibec response).

Recommendations on security and incident reporting obligations

3. **Work towards regulatory simplification: Develop technical measures to simplify reporting and decrease administrative burden;[8] Provide guidance on the interplay between the Electronic Communications (Security Measures) Regulations 2024 and NIS2; Provide guidance on the interplay between NIS2 and GDPR.**

In addition to NIS2, many entities in Ireland are (or will be) subject to other reporting requirements under EU laws like Regulation (EU) 2016/679 (General Data Protection Regulation) (the "GDPR"), the forthcoming Critical Entities Resilience Directive, and sector-specific legislation, with one incident potentially requiring reporting to various authorities at different time intervals. Recital 106 NIS2 acknowledges the existence of multiple reporting regimes and provides for the development of technical measures, including a single entry point for reporting, in order to simplify reporting and decrease administrative burden. We call on Government to make advances in this area.

The Communications Regulations and Digital Hub (Amendment) Act 2023 (the "2023 Act") transpose Articles 40 and 41 of the European Electronic Communications Code (the "Code"), which form the legal basis for the security measure provisions in the 2023 Act (including the draft Electronic Communications (Security Measures) Regulations 2024 which are being implemented thereunder). Article 40 and 41 of the Code are revoked by NIS2 and overtaken by the detailed security obligations in NIS2 (and relevant national implementing measures including the Bill). Subjecting electronic communications operators to two parallel security measures regimes and two parallel security incident notification regimes will impose a disproportionate regulatory burden. We therefore call for guidance on the interplay between the Electronic Communications (Security Measures) Regulations 2024 and security and incident notification requirements stemming from NIS2.

4. **Ensure cyber risk management and incident notification obligations offer flexibility, are technically feasible, aligned at EU level, and applicable in a manner proportionate to the varying risk profiles of essential and important entities.**

Head 29(7) provides for possible future Regulations further detailing the types of cyber security risk management measures to be taken. Consistency at EU level regarding these additional measures is important so that entities established and/or providing services in more than one Member State do not face a fragmented regulatory landscape and barriers to scaling in the Single Market.

5. **Develop guidance on the practical application of requirements to manage supply chain security.**

At present, Head 29(d), transposing supply chain risk management requirements, is liable to generate significant legal uncertainty given the lack of clarity surrounding allocation of responsibility between users and direct providers/suppliers. Consider the

[8] As provided for in Recital 106 NIS2.

development of NIS2-compliant contractual clauses to clarify minimum cyber security requirements for direct providers/suppliers.

Recommendations on supervision, enforcement and penalties

6. **Clarify the process for notifying Competent Authorities of the designation of Ireland as the country of main establishment under NIS2 (for entities in the digital infrastructure, digital provider and ICT risk management (B2B) sectors); Develop guidance for cross-border entities that are established in Ireland but do business in other jurisdictions (and vice-versa).**

Practical questions around registration and designation of Ireland as the country of main establishment under NIS2 (for entities in the digital infrastructure, digital provider and ICT risk management (B2B) sectors) require clarification, particularly as the 18 October application deadline approaches. National Competent Authorities should also begin engaging with Essential and Important entities before the National Cyber Security Act is signed into law to coordinate on compliance plans and inform them of their supervisory approaches.

7. **Ensure that entities supervised in Ireland face the same enforcement measures as in any other EU country; Avoid gold-plating.**

In cases of non-compliance with the law, the EU NIS2 text (Article 32) gives Member States powers to: (1) restrict management board members from their positions in essential entities and (2) suspend licenses from essential entities that are issued with licenses to operate their business in the State until they comply with NIS2 (Article 32(5)). Head 37B(1)(b) extends these enforcement powers to cover important entities too, with no accompanying explanatory note. Unjustified departures from the EU text should be avoided so that important entities in Ireland do not face undue regulatory burdens. This is also crucial to safeguard Ireland's competitiveness and ensure it remains an attractive place for companies to do business. In general, we urge that communication and 'in good faith' cooperation between entities and supervisors should be the primary route to achieving NIS2's goals rather than penalties and administrative sanctions.

8. **Ensure regulators possess sufficient capacities and resources to carry out their duties under NIS2.**

We welcome the funding allocated in Budget 2025[9] to the continued expansion of the NCSC, as called for by Ibec in our pre-Budget submission.[10] However, many sectoral regulators listed under Head 17 will supervise in the cyber security domain for the first time and should also be resourced accordingly. We welcome the explanatory note under Head 18 detailing NCSC guidance and support for other regulators under NIS2. Sectoral regulators must begin engaging with the Essential and Important entities under their supervision now to ensure that NIS2 compliance plans are feasible, predictable and proportionate.

9. **Ensure levies are proportionate and take account of the financial costs that will be absorbed by entities in preparing for NIS2 compliance.**

[9] DECC (2024) Press release on Budget 2025
[10] Ibec (2024) Sharpening our Edge

The Scheme amends the Communications Regulation Act 2002 to allow ComReg to extend its levy funding to its function under NIS2, suggesting that ComReg will impose a levy on organisations in the sectors under its supervision (Digital Infrastructure, ICT Service Management, Space and Digital Providers). The scheme also provides a legal basis for other Levy funded Departments and agencies to extend their levy model to activities under the Directive. In imposing levies, Competent Authorities must consider the additional costs borne by entities in scope of NIS2 e.g. costs associated with engaging with the audit process (for essential entities).

Recommendation on the National Cyber Security Centre

10. Clarify criteria for the exercise of NCSC powers in the interests of national security

The NCSC has a central role to play in raising Ireland's cyber resilience and coordinating national implementation of NIS2. We welcome recognition of this in the Bill, which establishes the NCSC on a statutory footing and grants it powers to fulfil its duties. While acknowledging the functions assigned to the NCSC under Head 3, we call for further clarity on the criteria for exercising the power under point (1)(d) to *"deny the use of network and information systems in the State to acts of foreign or domestic interference that are, or are intended to be, detrimental to the interests of the State or its international relations or are clandestine or deceptive or involve a threat to any person, device or essential service."* While recognising the imperative of national security, this function should only be invoked in a limited set of clearly defined circumstances. Such circumstances should be informed by a published set of objective, transparent, risk-based, technical criteria upon which a decision would be based. Considerations could include:

- Governance in the decision-making process;
- The necessary weight of evidence behind those criteria;
- The amount of notice that would be provided before function (d) would be invoked;
- The length of time that such a denial of service could last;
- The objective transparent criteria for the lifting of the denial of service;
- The mechanism by which a company could appeal a decision under function (d); and
- Recourse to companies affected by any denial unlawfully imposed.

Other comments

Head 2: The definition of ‘management board’ is unclear. We would welcome clarification of whether the definition corresponds to statutory Directors or is also intended to allow delegation to an Executive Board.

Head 23: This Head concerns the exclusion of local government and educational institutions from the scope of NIS2, noting that the Minster will be empowered to do so, pending an inter-agency risk assessment. When considering the final text of the Bill, we would urge the Department to consider the significant challenges and costs that NIS2 poses, especially for smaller local authorities. It is crucial that the implementation of the directive is proportionate and risk-based, considering the capacity and risk profile of different local authorities. We note that Germany, Hungary, Belgium, and Austria have excluded smaller local authorities from the scope of their transposing laws.

Head 28: The Explanatory Note accompanying this Head refers to the concept of gross negligence, which is not a well-developed legal concept in Irish law. We suggest that the language referred to in Head 43, with respect to connivance, be included as the sole nexus for officer liability, rather than including the reference to gross negligence, with respect to director’s liability.

Head 30: It is important to note that a requirement to use only certified products and services requires that a mature certification system with several certified suppliers is available. Otherwise, this provision could have the effect to concentrate and distort the market for supply of these products and services, driving increased costs to users.

Head 36: There should be a “reasonableness” check on the powers granted under this Head to ensure they are used in a proportionate manner.

Head 37B: In this Head, concerning penalties for non-compliance with a Compliance Notice, there appears to be ambiguity between Head 37B 1(a) (relating to penalties for non-compliance with a Compliance Notice) and the related Explanatory Note, specifically around "*other senior managers.*" The Head refers to “*any natural person who is responsible for discharging managerial responsibilities at chief executive officer or who is a director of the Essential Entity....within the meaning of the Companies Act 2014 as amended*.”, however the corresponding explanatory note refers to “*the power to restrict company CEOs and Directors and other senior managers*”. Clarity is required here.

Head 43: In ascertaining where personal liability could sit, where an act of a body corporate is proven to have been with the consent/connivance of or otherwise due to wilful neglect of a director, manager, secretary or other office of the body corporate (or person purporting to act in such capacity), that person is liable and subject to the same punishment as the body corporate. The same applies to a body corporate's "members" (i.e. shareholders). It is unclear whether this encompasses comparable fine levels, and this should be clarified.

Head 44:

- **B(4)**: This relates to the publication and corresponding redaction of grounding documentation for a notice of suspected non-compliance, using the phrase "*or for any other good and sufficient reason*" in relation to decisions in the discretion of the Competent Authority. This is a broad discretion which would benefit from clarification.
- **E**: This relates to publication of notices of suspected non-compliance. We recommend that non-compliance be finally and fully determined before it is made public.
- **F(2)(a)**: Where a notice of suspected non-compliance has been served, the essential entity can submit a proposal in writing in relation to measures to address the breach, which the Competent Authority can opt to publicly consult on. We question whether a public consultation is appropriate in an active investigation over suspected non-compliance.
- **L(1)**: The Competent Authority can provide copies of documents provided to them under this Head (and numerous others) to *"such other persons as [it] considers appropriate."* We believe this discretion is too broad and should be limited to the extent required in furthering the objectives of the relevant Head.

Head 45: This Head expresses an intention as opposed to a definitive solution and will require amending in the final Bill.

Ibec
For Irish Business

