Tithe an Oireachtais
Houses of the Oireachtas

An Comhchoiste um Dhlí agus Ceart, Gnóthaí Baile agus Imirce

Tuarascáil maidir leis an nGrinnscrúdú Réamhreachtach ar Scéim Ghinearálta an Bhille um Chibearshlándáil Náisiúnta 2024

Feabhra 2026

Joint Committee on Justice, Home Affairs and Migration

Report on Pre-Legislative Scrutiny of the General Scheme of the National Cyber Security Bill 2024

February 2026

34/JC/09

Contents

Committee Membership **4**

Cathaoirleach's Foreword **5**

1. Recommendations **6**

2. Overview of the Committees' Consideration **9**

2.1 Introduction 9
2.2 Purpose of the Bill 9
2.3 Procedural basis for scrutiny 9
2.4 Engagement with Stakeholders 9

3. Summary of Written Submissions **11**

3.1 Introduction 11
3.2 Key Issues raised in the submissions 11

1. Power of the NCSC to deny the use of network and information systems in the State (Head 3) 12
2. General powers of the NCSC (Part 2) 14
3. Transposition of the NIS2 Directive (multiple Heads) 17
4. Supervision and enforcement (Head 17 and Part 8) 18
5. Security and incident reporting obligations (Heads 11 and 29) 19

4. Summary of Oral Evidence **20**

4.1 Introduction 20
4.2 Key Issues raised in oral evidence 20

1. Cybercrime and ransomware (multiple Heads) 20
2. National security, and powers to deny usage of networks (Head 3) 23
3. Scanning and surveillance (Heads 6-10) 25
4. Implementation of NIS2, and sector opportunities 27

Appendix 1 – Opening Statements and Written Submissions **29**

Appendix 2 – Committee information **30**

Committee Membership

Cathaoirleach

Matt Carthy TD, Sinn Féin

Leaschathaoirleach

Paula Butterly TD, Fine Gael

Members

Tom Brabazon TD, Fianna Fáil

Catherine Callaghan TD, Fine Gael

Albert Dolan TD, Fianna Fáil

Gary Gannon TD, Social Democrats

Alan Kelly TD, Labour

Pádraig O'Sullivan TD, Fianna Fáil

Mark Ward TD, Sinn Féin

Senator Robbie Gallagher, Fianna Fáil

Senator Garret Kelleher, Fine Gael

Senator Michael McDowell, Independent

Senator Anne Rabbitte, Fianna Fáil

Senator Lynn Ruane, Independent

Cathaoirleach's Foreword

In July 2025, the Minister for Justice, Home Affairs and Migration, Mr Jim O'Callaghan TD, forwarded the General Scheme of the National Cyber Security Bill 2024 to the Joint Committee on Justice, Home Affairs and Migration in accordance with Standing Orders for the purpose of pre-legislative scrutiny.

This General Scheme seeks to transpose the NIS2 Directive into Irish law. The Scheme also provides for the establishment of the National Cyber Security Centre (NCSC) on a statutory basis.

The Committee welcomes certain aspects of this legislation, such as provisions to better tackle cybercrime, and the establishment of the NCSC on a statutory basis.

However, following its hearings on the General Scheme, the Committee wishes to highlight several areas which are of concern to the Committee, such as the potential for the power to deny network access to cause public disruption, and that the provisions for scanning under Heads 8 and 9 appear to run contrary to Article 8 of the ECHR, the GDPR and the Charter of Fundamental Rights of the European Union.

In undertaking pre-legislative scrutiny, the Committee has sought to scrutinise the proposed legislation and provide recommendations on areas where it believes change or amendments are warranted. Among the areas identified for further examination within the General Scheme include allowing for a grace period following the implementation of the proposed legislation, ensuring safeguards on the powers of the NCSC, and increasing the guidance available to affected stakeholders.

The Committee has made a number of recommendations, and a copy of this report will be sent to the Minister for Justice, Home Affairs and Migration. I would like to express my appreciation to all the stakeholders for their contributions and to the Members of the Committee for their engagement on this subject.

Finally, I hope that this report will help to inform the legislative process and make a valuable contribution to the forthcoming legislation.

Matt Carthy TD

Cathaoirleach

18 February 2026

1. Recommendations

1. The Committee recommends that Head 3(1)(d) be removed in its entirety. If it is necessary to retain a power to deny network access in exceptional circumstances, the Committee recommends that such a power be subject to the following:
    - objective criteria,
    - procedural fairness,
    - temporal and substantive limits,
    - independent oversight, and
    - the application of supervision and enforcement provisions.

2. The Committee recommends that Head 6 be amended to provide that the National Cyber Security Centre may scan networks only with the consent of the relevant entity, except in relation to essential or important entities. The Committee further recommends that if the aim behind this Head is to permit widespread scanning, then it should be redrafted to make this clear, to require independent authorisation of such scanning based on explicit criteria, and to explain how such scanning would be subject to safeguards to ensure that it is limited to what is necessary and proportionate.

3. The Committee recommends that Head 7 be removed, and that any measure regarding blocking or domain name suspension be redrafted in accordance with the requirements of the European Convention on Human Rights.

4. The Committee recommends that Head 8 be redrafted to limit it to significant threats or risks, to limit the retention of data to that which is both necessary and proportionate to such risks, and to limit the retained data to metadata only unless it is shown that it is necessary to retain a particular category of content data, in which case the retention of content data should be limited to that category of data.

5. The Committee recommends that Head 11 be amended to provide for a requirement to report incidents, where they occur in circumstances which fall within the remit of An Garda Síochána.

6. The Committee recommends that Head 15 be amended to include an obligation on entities to report to An Garda Síochána all intrusion or interference incidents that impact on the provision of their service without delay.

7. The Committee recommends that Head 26 be amended to include an obligation on entities to report to An Garda Síochána all incidents covered by subhead 2.

8. The Committee recommends that Head 29 be amended to 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.

9. The Committee recommends Head 29 be amended to develop guidance on the practical application of requirements to manage supply chain security.

10. The Committee recommends that Head 33 be amended to include an obligation or duty on An Garda Síochána and the National Cyber Security Centre to share information relating to modes of compromise, threat actors, techniques, alerts and vulnerabilities, in order to enhance the capacity to respond and prevent cyber incidents or compromise.

11. The Committee recommends that Head 37C be amended to define members of An Garda Síochána in their capacity on inspections or searches.

12. The Committee recommends that a transition or grace period of 12 months should be provided from the date of commencement of the legislation, to ensure that all stakeholders have adequate time to prepare for compliance, to bring their operations, policies and procedures in line with the requirements.

13. The Committee recommends that the legislation includes explicit provisions to ensure that any action taken under its powers does not inadvertently disrupt critical infrastructure or essential services, particularly where such disruption could have serious consequences for public health, safety, or the functioning of the State.

14. The Committee recommends that the National Cyber Security Centre should be required to publish annual reports detailing the exercise of its powers, including the number and nature of any denials of network access, the grounds for such actions, and the outcomes of any appeals or reviews.

15. The Committee recommends that the proposed legislation provides for ongoing consultation and engagement with stakeholders, including industry, civil society, and technical experts, to ensure that its implementation remains responsive to evolving threats and technological developments.

16. The Committee recommends that the legislation works towards regulatory simplification by developing technical measures to simplify reporting and decrease administrative burden, and by providing guidance on the interplay between the Electronic Communications (Security Measures) Regulations 2024 and the NIS2 Directive, and NIS2 and GDPR.

2. Overview of the Committees' Consideration

2.1 Introduction

This is the report on pre-legislative scrutiny of the General Scheme of the National Cyber Security Bill 2024, which was approved by the Government of the 33rd Dáil on the 24th of July 2024.

The Joint Committee on Transport and Communications (JCTC) of the 33rd Dáil were originally requested to undertake pre-legislative scrutiny of the General Scheme. However, pre-legislative scrutiny was not completed before the dissolution of the 33rd Dáil. In November 2024, JCTC stopped its work on the scrutiny of the General Scheme and forwarded the submissions it had received to Minister of State Ossian Smyth. The cyber security function was transferred to the Department of Justice, Home Affairs and Migration in June 2025.

The Joint Committee on Justice, Home Affairs and Migration was requested to undertake pre-legislative scrutiny of the General Scheme on 2nd July 2025.

2.2 Purpose of the Bill

The General Scheme consists of 49 Heads. The proposed legislation seeks to be the legislative vehicle for the transposition of the Network and Information Security Directive EU 2022/2555 (NIS2 Directive) into Irish law, and to provide for the establishment of the National Cyber Security Centre (NCSC) on a statutory basis and for related matters.

2.3 Procedural basis for scrutiny

Pre-legislative consideration was conducted in accordance with Standing Order 181 which provides that the General Scheme of all Bills shall be given to the Committee empowered to consider Bills published by the member of Government.

2.4 Engagement with Stakeholders

The Joint Committee on Justice, Home Affairs and Migration invited submissions from stakeholders on the National Cyber Security Bill 2024. A list of the submissions received is provided in Appendix 1.

On 25 November 2025, the Committee held a public engagement with several of these stakeholders. A link to the full transcript of the engagement can be found here.

The full list of witnesses that attended the meeting is available below.

Stakeholders	Capacity
Individual ▪ Mr Sean McElligott	Witness
An Garda Síochána (AGS) ▪ Mr Barry Walsh, Detective Chief Superintendent ▪ Mr Pat Ryan, Detective Superintendent	Witnesses
Digital Rights Ireland (DRI) ▪ Dr TJ McIntyre, Chair	Witness
Irish Council for Civil Liberties (ICCL) ▪ Ms Olga Cronin, Senior Policy Officer	Witness
Ibec ▪ Mr Erik O'Donovan, Head of Digital Economy Policy ▪ Ms Áine Clarke, Digital & AI Policy Executive	Witnesses
Department of Justice, Home Affairs and Migration ▪ Mr David McGill, Principal Officer ▪ Ms Clare Heenan, Assistant Principal Officer	Advisors

3. Summary of Written Submissions

3.1 Introduction

A summary is provided in section 4.2 of the key issues raised in the submissions received, in relation to the General Scheme.

The Committee received submissions from the following stakeholders:

- Ibec
- Mr Sean McElligott
- Digital Rights Ireland (DRI) and Irish Council for Civil Liberties (ICCL)
- An Garda Síochána

3.2 Key Issues raised in the submissions

The following issues were common to multiple submissions received:

1. Power of the NCSC to deny the use of network and information systems in the State (Head 3).
2. General powers of the NCSC (Part 2).
3. Transposition of the NIS2 Directive (multiple Heads).
4. Supervision and enforcement (Head 17 and Part 8).
5. Security and incident reporting obligations (Heads 11 and 29).

1. Power of the NCSC to deny the use of network and information systems in the State (Head 3)

- Ibec welcomed recognition in the General Scheme that the National Cyber Security Centre (NCSC) has a central role to play in raising Ireland's cyber resilience and coordinating national implementation of NIS2.

- Ibec called for further clarity on the criteria for exercising the power under Head 3(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."*

- Ibec believed that this function should only be invoked in a limited set of clearly defined circumstances, informed by objective, transparent, risk-based, technical criteria upon which a decision would be based. Ibec believed these criteria 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 this function or power 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 this function or power, and
  - recourse to companies affected by any denial unlawfully imposed.

- Mr Sean McElligott echoed Ibec's concerns about the provision under Head 3(1)(d), and stated that this provision is not mirrored in the NIS2 Directive and appears to be unique to the Irish legislative approach.

- Mr McElligott cited vague and highly subjective grounds for exercising this power as a key concern with the subhead, and was of the view that this could create a risk of arbitrary or inconsistent application, undermining legal certainty and the principle of proportionality.

- Mr McElligott pointed to an absence of procedural safeguards in this subhead, highlighting that the power under Head 3(1)(d) may be exercised unilaterally by the NCSC without any requirement for judicial or independent oversight, prior notice, or opportunity for affected parties to make representations.

- Mr McElligott was concerned that the power conferred by this subhead could be invoked in response to relatively minor incidents, and could lead to the disruption of

critical infrastructure, the operations of both domestic and international entities, and essential services, such as healthcare, energy, and transportation, with attendant risks to public safety and economic stability.

- Another concern that was indicated by Mr McElligott was the potential of the power provided for in this subhead to deter foreign direct investment in Ireland's digital infrastructure and undermine confidence among multinational operators, pointing to the absence of comparable provisions in other EU Member States.

- Expanding on the lack of an equivalent power in the legislation of other Member States, Mr McElligott considered that Ireland may be seen as an outlier, and potentially exposing the State to legal challenge and reputational risk.

- Mr McElligott called for the complete removal of Head 3(1)(d) from the General Scheme. Should this not be undertaken, Mr McElligott suggested that safeguards are introduced regarding the powers set out in the subhead, including:
    - objective criteria for invocation,
    - procedural fairness by the NCSC,
    - temporal and substantive limits for the denial of access,
    - oversight by the High Court, or another independent body of the powers being exercised, and
    - the extension of supervision and enforcement provisions, set out in Part 8, to these powers.

2. General powers of the NCSC (Part 2)

The submission received from Mr Sean McElligott, and the joint submission from Digital Rights Ireland (DRI) and the Irish Council for Civil Liberties (ICCL), include concerns regarding the powers that will be conferred to the NCSC by Part 2 of the General Scheme.

Mr McElligott believed that certain provisions, particularly in Part 2 relating to the powers of the NCSC, raise substantial concerns regarding the scope, subjectivity, and lack of procedural safeguards, while the joint submission by DRI and ICCL raises detailed concerns about the provisions within Heads 6 to 10 of the General Scheme. DRI and ICCL prefaced their submission by emphasising that the NCSC is not an independent body, as Head 3 provides that it is 'under the authority of the Minister'.

- DRI and ICCL believed that the provision within Head 6 that permit the NCSC to scan any publicly accessible network or information system in the State for vulnerabilities, without notifying the owner or seeking their consent, goes beyond the requirements of NIS2.

- DRI and ICCL pointed to the requirements of NIS2, which requires Computer Security Incident Response Teams (CSIRTs) to have powers to scan essential or important entities only, and underlined that Head 6 would allow the NCSC to scan networks belonging to entities such as small businesses, political parties, and home networks.

- DRI and ICCL called for the amendment of Head 6 to provide that the NCSC may scan networks only with the consent of the relevant entity, except in relation to essential or important entities, or that if the Head's aim is to permit widespread scanning, then it should require independent authorisation of such scanning based on explicit criteria, and to explain how such scanning would be subject to safeguards to ensure that it is limited to what is necessary and proportionate.

- The submission from DRI and ICCL highlighted the wide and uncertain scope of the powers that Head 7 would create, stating that while the title of the Head refers to 'DNS blocking and sinkholing', subhead 7(2) refers to 'appropriate measures' to be taken by both DNS providers and domain registrars, going beyond what is referred to in the title of the Head, and would allow the suspension or revocation of a domain name.

- DRI and ICCL described these measures as a potential internet death penalty for a particular domain name. The submission also highlighted that DNS blocking is also extremely likely to cause over-blocking by cutting off access to unrelated material which happens to be hosted on the same domain name, affecting third party rights.

- DRI and ICCL were of the view that DNS blocking and domain name suspension raise significant issues for the right to freedom of expression, as well the rights of businesses who may find their websites inaccessible through no fault of their own.

- DRI and ICCL stated in their submission that Head 7 does not adhere to the requirements of the 2018 Recommendation on The Roles and Responsibilities of Internet Intermediaries by the Committee of Ministers of the Council of Europe, and pointed out that NIS2 does not require that the NCSC be given blocking powers.

- DRI and ICCL called for Head 7 be withdrawn, and that any measure regarding blocking or domain name suspension be redrafted in accordance with the requirements of the European Convention on Human Rights.

- DRI and ICCL emphasised the extent to which the provisions within Head 8 would be privacy invasive. Their submission remarked that these provisions would permit the NCSC to collect the entirety of the network traffic in public sector bodies, all metadata about private communications carried on public electronic communications networks, and private communications carried on social network providers, information which could then be stored for up to 18 months.

- DRI and ICCL pointed out that while the provisions set out in Head 8 require the consent of the 'entities concerned', they do not require the consent of the individuals affected. Their submission underlined that Head 8 enables bulk collection of data relating to all employees, visitors, users and Irish residents in general, and that there is no requirement in the Head that the use of such a system be proportionate.

- DRI and ICCL suggested that the powers under Head 8 would be contrary to the requirements of Article 8 of the European Convention on Human Rights as well as the requirements of the GDPR and the ePrivacy Directive.

- DRI and ICCL were of the view that the provision in Head 8(3), which appears to create a purpose limitation principle in relation to data collected, is undermined by Head 10(1), which permits processing of personal data for purposes other than those for which the data was collected, and by Head 11 which permits information sharing with the Garda Síochána.

- DRI and ICCL called for Head 8 to be redrafted to limit it to significant threats or risks, to limit the retention of data to that which is both necessary and proportionate to such risks, and to limit the retained data to metadata only unless it is shown that it is necessary to retain a particular category of content data.

- DRI and ICCL underlined concerns relating to the creation through Head 9 of a compulsory surveillance power which can extend to the telephony and internet use of the entire population.

- Their submission indicated that Head 9 is considerably more invasive than the Communications (Retention of Data) Act 2011 in that it can require providers to install surveillance devices on their networks, restricting their ability to monitor or challenge state surveillance, and that that Head does not provide that the use of these mass surveillance powers should be proportionate to the threat.

- DRI and ICCL submitted that as the provisions of Head 10 appear unclear, imprecise and unforeseeable, they risk leading to a disproportionate interference with individuals' fundamental rights to privacy and data protection.

- Their submission was concerned that the wording of Head 10(2)(b) is overly broad and insufficiently defined, risking unjustified processing of people's highly sensitive personal data, and that the specific conditions and safeguards for the processing of special category data, provided for in Article 9(2)(g) GDPR, are entirely absent from this Head.

3. Transposition of the NIS2 Directive (multiple Heads)

- Mr Sean McElligott highlighted that the General Scheme does not provide for a transition or grace period to allow stakeholders to prepare for the new regulatory requirements resulting from the transposition of the NIS2 Directive.

- Mr McElligott believed that the fundamental shift in the regulatory landscape for cyber security in Ireland resulting from the transposition of NIS2 would be comparable in scale and complexity to the introduction of the GDPR.

- In his submission, Mr McElligott referenced the grace period provided to facilitate orderly and effective implementation of the GDPR. Mr McElligott called for a transition or grace period of six to twelve months to be provided from the date of commencement of the proposed legislation, to ensure that all stakeholders have adequate time to prepare for compliance and will reduce the risk of inadvertent breaches and associated enforcement action, which was echoed by Ibec.

- Ibec called for a transition or grace period of one year from the date the proposed legislation is signed into law, to allow organisations to review their cyber security posture, prepare compliance plans, and provide appropriate updated training to employees.

- Mr McElligott underlined that, under NIS2, the country of origin is not more important than the implementation of active cyber protection requirements. The submission went on to suggest that if the Government steers cyber resilience based on subjective criteria, the result is the opposite of what NIS2 aims to achieve.

- Mr McElligott asserted that the General Scheme should provide for ongoing consultation and engagement with stakeholders, including industry, civil society, and technical experts, to ensure that its implementation remains responsive to evolving threats and technological developments, and remarked that implementation must avoid creating unnecessary burdens for businesses, hindering their ability to innovate and compete.

- Ibec pointed to the important role to be played by the State under NIS2, supervising many global entities in the digital infrastructure and digital provider sectors on a pan-European basis. Ibec stated that Ireland's growing cyber security industry also stands to benefit from increased state capacity in this area.

- Ibec listed the demonstration of leadership in digital policy and regulation as a priority, given the investment that could be attracted.

4. Supervision and enforcement (Head 17 and Part 8)

- Ibec indicated that 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.

- Ibec called for national Competent Authorities to begin engaging with essential and important entities before the proposed legislation is enacted, to coordinate on compliance plans, and inform them of their supervisory approaches.

- Ibec considered that guidance should be developed for cross-border entities that are established in Ireland but do business in other jurisdictions, and *vice-versa*.

- In its submission, Ibec discussed Article 32 of the NIS2 text, and stated that Head 37B(1)(b) extends the enforcement powers provided for by Article 32 to cover important entities as well.

- Ibec emphasised that the Head should avoid unjustified departures from the EU text so that important entities in Ireland do not face undue regulatory burdens, and stressed the importance of safeguarding Ireland's competitiveness and ensure it remains an attractive place for companies to do business.

- Ibec called for the adequate resourcing of sectoral regulators listed under Head 17, as many of these will supervise in the cyber security domain for the first time, and submitted that 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.

- In its submission, An Garda Síochána (AGS) discussed Head 37C(1)(a), enquiring whether the functions of its members are to search or inspect, or to accompany NCSC Authorised Officers in order to prevent a Breach of the Peace or other obstructive actions. AGS called for its members to be defined in their capacity on inspections or searches.

- AGS noted that powers under Criminal Justice Legislation allow for its members to seize and retain items of evidential importance, and that these broader powers may cover the provisions set out in Head 37D.

5. Security and incident reporting obligations (Heads 11 and 29)

- Ibec welcomed the provision in Head 29(7) for possible future Regulations regarding the types of cyber security risk management measures to be taken.

- Ibec stressed the importance of consistency at EU level regarding these additional measures 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.

- However, Ibec believed that Head 29(d), which transposes 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.

- Ibec called for guidance to be developed on the practical application of requirements to manage supply chain security, and for NIS2-compliant contractual clauses to be developed to clarify minimum cyber security requirements for direct providers/suppliers.

- An Garda Síochána (AGS) pointed to the provisions in Head 11, for the sharing of data between NCSC and AGS/Data Protection Commission, including personal data which would be of assistance in its investigations. AGS suggested that where an incident has occurred, in circumstances which falls within the remit of AGS, it is required that such an incident is reported.

4. Summary of Oral Evidence

4.1 Introduction

In the course of the public hearing on 25th November 2025, a number of important points were raised.

A summary of the main areas discussed in evidence to the Committee follows.

4.2 Key Issues raised in oral evidence

1. Cybercrime and ransomware (multiple Heads)

- During the engagement, An Garda Síochána (AGS) spoke about cybercrime and ransomware, in the context of the proposed legislation outlined in the General Scheme. AGS believed that the beneficial impacts of the NIS2 Directive, and its transposition into Irish law through the proposed legislation, are most welcome as mechanisms to create a more secure cyber ecosystem.

- AGS told the Committee that it is estimated that the cybercrime economy will be worth just over €9 trillion by the end of 2025, up from an estimated €5.5 trillion in 2020. When the Committee enquired about the composition of these sums, AGS agreed that it was a mixture of an increased number of instances, increased value, and newly designated cybercrime. AGS stated that economic fraud forms the vast majority of cybercrime in terms of global monetary value.

- AGS stated that of cyber-dependent crimes, which represent the greatest threat of societal level disruptions, ransomware is the most significant threat, pointing to the cyber attack on the HSE in 2021. AGS pointed to the added cost of the mitigation and remediation elements of a ransomware attack.

- AGS commented that there is evidence of nation-state involvement in cybercriminality. When asked by the Committee to expand on this point, AGS added that countries are involved in various types of warfare, who are excluded from the normal global ecosystem, employing cyberwarfare and cyberattacks as a mechanism both to generate income and to disrupt nation-state services.

- The Committee enquired about the extent of collaboration with international partners in this area, particularly EU member states. AGS explained that there is extensive collaboration, that it is an active participant in a lot of Europol activities and have a presence in all meetings Europol has in this area, and that it attended the Interpol working group meeting on cybercrime in November 2025.

- When asked by the Committee about the impact of cybercrime at a local level, and the importance of implementing this legislation, AGS highlighted the experiences of small or medium enterprises (SMEs), stating that cybercrime causes real harm and it is real people who are impacted.

- The Committee asked the witnesses whether essential service operators should be permitted to plan for, or pay, ransoms, and whether this should be made explicit in the proposed legislation. Mr Sean McElligott conveyed that resources should instead be directed into chasing down the perpetrators of ransom attacks.

- AGS acknowledged that while there is a big debate going on as to whether payment of ransom should be legislated for, it did not believe that it falls into the context of this General Scheme.

- AGS added that it does not advocate payment of ransoms, as victims are dealing with criminals who are intent on maximising the payout they can extract from the victim, particularly criminals who are probably resident in other jurisdictions. Ibec agreed with this assessment by AGS, and echoed Mr McElligott's suggestion that resources should be focused on stopping the criminals.

- Ibec underlined the need to build up cyber-resilience by directing part of the National Training Fund towards digital skills, building the capacities of the State's indigenous cyber sector and the National Cyber Security Centre (NCSC). Ibec reiterated the need to invest in cyber readiness and boosting digital literacy across the whole population.

- Digital Rights Ireland (DRI), appearing in front of the Committee alongside the Irish Council for Civil Liberties (ICCL), spoke about the link between the origins of ransomware and cryptocurrency. DRI stated that the most effective solution to minimise ransomware would be to crack down on cryptocurrencies, adopt proper controls on exchanges, and eliminate certain exchanges entirely.

- When asked by the Committee to expand on the link between those involved in establishing cryptocurrency and ransomware, DRI stated that the only way ransom can be paid at scale is by using some form of cryptocurrency.

- The Committee asked AGS about mandatory reporting obligations through the General Scheme. AGS highlighted that from its perspective, there is not currently any mandatory reporting obligation, though it would see a huge value in having mandatory reporting in order to get a better global picture of cybercrime. AGS added that there is significant under-reporting of cybercrime.

- AGS told the Committee that it welcomed this legislation as it is orientated towards prevention, which it believed is the best form of attack, indicating that AGS did not want to be the reactive element of the State showing up to a cybercrime as it is too late at that point and the damage has been done.

2. National security, and powers to deny usage of networks (Head 3)

- Mr McElligott underlined the breadth and subjectivity of head 3(1)(d), pointing to the power allowing the regulator to deny the use of network and information systems on certain grounds, noting that this power does not appear in the NIS2 directive. Mr McElligott stated that without objective criteria, clear thresholds and procedural safeguards, this power risks arbitrary or inconsistent application with unforeseen consequences and significant practical risks.

- Mr McElligott emphasised that modern networks underpin hospitals, electricity grids, and transport systems, and stated a sweeping denial of access, even if intended to address a discrete issue, could inadvertently cascade into outages of essential services with consequences for public safety and economic stability.

- Mr McElligott suggested that consideration should be given to either removing Head 3(1)(d) altogether or, if a denial power is indispensable for truly exceptional cases, it should be tightly constrained by law, grounded in published, objective criteria, so that actions taken under the General Scheme do not inadvertently disrupt essential services and that a regime that is both resilient and proportionate is delivered.

- DRI echoed Mr McElligott's concerns with proportionality in the application of powers under Head 3, stating that the Head would allow the NCSC to block access to social network X in Ireland if it was of the view individuals were using it to stir up racism, hatred and attacks on migrants in the State, asserting that these powers should have appropriate oversight and safeguards.

- When responding to the Committee's request to expand on the conflict between what is proposed in Head 3(1)(d) and what is set out in the NIS2 directive, Mr McElligott similarly opined that this Head gives the NCSC the power to disconnect Amazon from the Irish network if it was subjected to a very serious hack. McElligott commented that it seems the NCSC has the power to do whatever it wants to whomever it wants whenever it wants without any regulatory supervision whatsoever, under the proposed legislation.

- When asked for its perspective by the Committee, the Department highlighted that Head 3 is very much about putting the NCSC on a statutory footing, and that disconnecting an entity from a network is a function as opposed to a power. The

Department added that it does not envisage that it will ever be used to just unilaterally compel anybody to disconnect somebody from a network.

- The Department explained that there are no compulsion powers in Head 3(1)(d), and that Heads 6 and 7 allow the NCSC to apply certain powers for certain, specific reasons, some of which is definitely overseen by the courts.

- DRI highlighted that under Head 7, there is the power to impose an Internet death penalty, on websites, services, IP addresses and other things on the Internet without a court order, without provision for independent oversight of the imposition of the Internet death penalty and without a clear appeals mechanism in place against the imposition of an Internet death penalty.

- When questioned by the Committee about the absence of independent or judicial control in the proposed legislation, the Department stated that there is judicial control for the powers under Head 9, and that the General Scheme will come under the examination of the Office of the Independent Examiner of Security Legislation.

- The Committee indicated that the reference to 'national security' within the General Scheme may not necessarily have to be cybersecurity, stating that national security, whether it is defined or undefined, is something much larger.

- The Committee enquired whether the General Scheme should be redrafted to ensure that the terms 'national security' or 'detrimental to the interests of the State' are not used to strangle freedom of expression.

- Mr McElligott agreed with these assessments, stating that technical standards and baselines should be put in place. Mr McElligott added that the legislation is not based on technical standards, but rather on other things, such as discrimination against the State, and described it as almost 'Big Brother-esque'.

- DRI commented that these provisions are domestic in nature, and not required under NIS2. DRI went on to suggest that a pure transposition of NIS2 would be better, and then decide to what extent additional national security powers should be included. DRI highlighted that Head 3 requires substantial revision if it is to be compliant with procedural safeguards that are required by the European Convention on Human Rights (ECHR).

3. Scanning and surveillance (Heads 6-10)

- DRI told the Committee that while it sees the General Scheme as an important step forward in transposing the NIS2 Directive, it is vital to avoid compromising cybersecurity in doing so, alluding to aspects of the proposed legislation which are purely domestic and not required for the transposition of the directive.

- DRI highlighted that while the Directive requires the regulator [the NCSC] to be given the power to scan networks for vulnerabilities only in the context of networks of essential and important entities, Head 6 goes well beyond that, permitting scanning without consent of networks of small businesses, NGOs, homes or politicians offices.

- DRI underlined two entirely unprecedented powers under Head 8, firstly drawing attention to the power to scan and store the entirety of the network traffic in public sector bodies, and also highlighting the power to allow the NCSC to do likewise. DRI stated that under this power, the NCSC could collect metadata about private communications on public networks, such as mobile phone and home broadband providers and messages sent via social media providers, and that this information could be stored by them for up to 18 months. DRI asserted that both powers could be used without the consent of any of the individuals affected, and gave the view that this is clearly in breach of European Court of Justice jurisprudence.

- DRI outlined its concerns with Head 9 allowing for the collection of metadata about communications in a similar way, but in this case on a compulsory basis. DRI believed that this power would allow the NCSC to compel providers, such as mobile phone operators, other network providers and data centre operators, to allow it to install equipment on their devices that could collect information about communications about every individual user of the service for an extended period of time without any individualised justification. DRI was concerned that while this would be done on the basis of national security grounds, 'national security' is not defined anywhere in the General Scheme.

- DRI was also concerned at the largely open-ended power on the part of the NCSC to share data, including for undefined national security reasons but without any clear limits on that power, in Head 10.

- The Committee was concerned that the General Scheme may veer into policy creep or something is happening that has little to do with cybersecurity and more to do with a wider surveillance that covers more than just cybersecurity vulnerabilities and threats. The Committee asked the witnesses whether the proposed legislation could be used to get particular data or access to WhatsApp or iMessages, which could then be used in other ways that were outside the remit of this General Scheme.

- Mr McElligott echoed concerns regarding policy creep, seeing it as being very applicable to this situation, stating that there are powers and functions that are extremely broad and would allow somebody to do basically whatever they wanted whenever they wanted to whomever they wanted. Mr McElligott indicated that he did not think that would work in practice because somebody would challenge it, and reiterated that the General Scheme goes way beyond the applicable Directive.

- DRI underlined that there is independent authorisation and, typically, judicial oversight at one stage or another regarding State surveillance in a normal context, and highlighted that Heads 8 and 9 run contrary to Article 8 of the ECHR, the GDPR and the Charter of Fundamental Rights of the European Union.

- When asked by the Committee why the piece on scanning for vulnerabilities without consent would be necessary, DRI explained that there are essential entities that are so important to society that it is important that we make sure they are functioning correctly, and we only give the agencies the power to proactively scan them without consent because we think they are too big to fail and we need to keep them under close regulation.

- The Committee asked the Department that, given the concerns raised by DRI and ICCL in their submission about the bulk data collection, the domain block and the installation of surveillance systems, can it state clearly how these provisions have been assessed for compliance with EU data protection law and the recent CJEU rulings.

- The Department responded by stating that the General Scheme only provides for interception of data, and it is on the networks and information systems of their actual networks to make sure they are not under threat. The Department added that regarding the oversight piece, it has submitted the General Scheme to the Data Protection Commission for its views and was still waiting for that to come back at the time of the meeting.

4. Implementation of NIS2, and sector opportunities

- Ibec described cybersecurity as an economic and social imperative and an opportunity for Ireland, particularly given that over 30% of EU data is hosted in the State. Ibec stated that cybersecurity is fundamental to safeguarding trust in the State's digitalised economy and protecting the State's critical infrastructure.

- Ibec drew attention to the significant impact of the NIS2 Directive on Irish business, stating that while fewer than 150 organisations were in scope of the first NIS Directive, it is estimated that over 4,500 organisations will be directly in scope of NIS2, with many more indirectly affected by the requirements on in-scope organisations to manage the cybersecurity of their supply chains.

- Ibec highlighted a lack of cybersecurity readiness, particularly among SMEs, which directly impacts the ability of businesses to understand and comply with their regulatory obligations, adding that almost one in four companies in Ireland has reported difficulties recruiting staff with the necessary cybersecurity skills.

- Ibec believed that the State simply does not have enough skilled professionals to meet the surge in demand the proposed legislation will create, and called for some of the €2 billion surplus of the National Training Fund to be directed towards cybersecurity and other digital skills.

- While Ibec strongly supported the continued expansion and resourcing of the NCSC, it highlighted that the General Scheme designates sectoral regulators, many of which will be supervising cybersecurity for the first time, and underlined that it is critical that these bodies are sufficiently resourced, not just with funding but with the technical experts needed to provide guidance to businesses.

- Noting the increase in cyber regulation in the EU, including NIS2, Ibec highlighted the significant opportunity for the growth of the State's cybersecurity sector, as more regulated entities will mean more demand for cybersecurity products and services. Ibec stated that the cybersecurity sector is already a major contributor to the Irish economy, comprising over 500 firms and generating €2.7 billion in annual revenue.

- In Ibec's view, the proposed legislation should align with the NIS2 text and avoid gold-plating for coherence and certainty. Ibec noted that many important details

necessary for complying with NIS2 have been omitted from the General Scheme, and called for any costs levied on organisations should also be proportionate and take into account the financial cost of complying with the law.

- When asked by the Committee to expand on the omissions from the General Scheme, Ibec stated that it does not know what is meant by the obligation on organisations to report significant incidents, and that there is no real information on the thresholds for classifying that kind of incident, nor are there templates for incident reporting. Ibec added that regarding the requirement on companies to manage their direct suppliers, guidance is needed on what that really looks like in order that they can actually comply.

- The Committee enquired about what a grace period for implementing compliance with the proposed legislation would look like in real terms. Ibec reiterated its call in its submission to the Committee for an additional 12 months, noting that the challenge for businesses is that they need to see the final text of the legislation. Ibec also suggested that this impacts our national ambition as a regulatory hub.

- Mr McElligott echoed Ibec's calls for a grace period, suggesting that an extension of six to 12 months after commencement would support orderly implementation across both regulated entities and competent authorities, much as a transition period did for GDPR.

- The Committee asked the Department whether an implementation period was under consideration. The Department stated that it is certainly under consideration, although it did not know how it can give legal effect to such a period. The Department added that it would need to get advice on that in terms of obligations to transpose the Directive and make sure it is operational. The Department emphasised that it and the regulator have always taken the approach that there will be a ramping-up period, and that guidelines will not be exactly mandatory from the start.

Appendix 1 – Opening Statements and Written Submissions

Opening Statements – meeting of 25th November 2025

Name of Stakeholder	Link to Opening Statement
Mr Sean McElligott	Opening statement
Ibec	Opening statement
Digital Rights Ireland and Irish Council for Civil Liberties	Opening statement
An Garda Síochána	Opening statement

Written Submissions

Name of Stakeholder	Link to Submission
Mr Sean McElligott	Submission
Ibec	Submission
Digital Rights Ireland and Irish Council for Civil Liberties	Submission
An Garda Síochána	Submission

Appendix 2 – Committee information

Publications

All publications for this committee are available on the Oireachtas website.

Committee videos

Footage of Committee proceedings can be found on the Committee videos page.

Committee debates

Transcripts of Committee debates can be found on the Committee debates page.

Contact details

The contact details for the Committee can be found on the Committee page.

Orders of reference

Read the Orders of reference for the Committee.