Submission to the Joint Committee on Justice, Home Affairs and Migration on the General Scheme of the National Cyber Security Bill 2024 ("the Bill")

1. Introduction

This submission is presented to the Joint Committee on Justice, Home Affairs and Migration as part of the pre-legislative scrutiny of the Bill.

The Bill seeks to transpose the NIS2 Directive and establish a robust framework for cyber security in Ireland which is a significant and timely legislative initiative. The establishment of the National Cyber Security Centre (NCSC) and the articulation of its statutory functions are welcomed by stakeholders, as they promise to enhance national resilience, facilitate information sharing, and improve incident response capabilities.

However, certain provisions within the Bill, and in particular those contained in Part 2 relating to the powers of the NCSC, raise substantial concerns regarding the scope, subjectivity, and lack of procedural safeguards. These concerns are most acute in relation to Head 3(1)(d), which confers upon the NCSC a sweeping and unilateral power to deny access to network and information systems. The following submission sets out a detailed analysis of these issues and proposes a series of amendments designed to ensure that the Bill achieves its objectives in a manner that is proportionate, transparent, and consistent with the rule of law and best international practice.

2. Head 3(1)(d): The Power to Deny Network Access – Need for Limitation, Clarification, and Oversight

Current Provision and Context:

Head 3(1)(d) of Part 2 of the Bill provides that the NCSC may "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." This provision is not mirrored in the NIS2 Directive and appears to be unique to the Irish legislative approach.

Key Concerns:

- **Vagueness and Subjectivity:** The grounds for exercising this power—such as "detrimental to the interests of the State," "clandestine or deceptive," or "threat to any person, device or essential service"—are highly subjective and lack clear, objective criteria. This creates a risk of arbitrary or inconsistent application, undermining legal certainty and the principle of proportionality.
- **Absence of Procedural Safeguards:** Unlike other intrusive powers in the Bill (for example, the deployment of network sensors under Head 9, which requires a High Court order), 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.
- **Potential for Disproportionate Impact:** The breadth of the power means it could be invoked in response to relatively minor incidents, with the potential to disrupt critical infrastructure, essential services, and the operations of both domestic and international entities. This could have severe consequences, including the interruption of vital services

such as healthcare, energy, and transportation, with attendant risks to public safety and economic stability.

- **Chilling Effect on Investment and Innovation:** The existence of such a broad and unchecked power may deter foreign direct investment in Ireland's digital infrastructure and undermine confidence among multinational operators, particularly given the absence of comparable provisions in other EU Member States.
- **Lack of Precedent in EU Law:** No equivalent power exists in the NIS2 Directive or in the legislation of other Member States, making Ireland an outlier and potentially exposing the State to legal challenge and reputational risk.

Recommended Amendments:

- **Complete Removal of Head 3(1)(d): In light of the above concerns, it is strongly recommended that Head 3(1)(d) be removed in its entirety. The provision's breadth, lack of objective criteria, and absence of procedural safeguards render it incompatible with fundamental principles of legal certainty, proportionality, and due process.**
- **Alternative Approach – Introduction of Safeguards: Should it be considered necessary to retain a power to deny network access in exceptional circumstances, the following amendments are proposed to ensure that any such power is exercised in a manner that is transparent, proportionate, and subject to appropriate oversight:**
  - **Objective Criteria:** The power should only be exercisable where there is a clear, imminent, and demonstrable threat to national security or the continued operation of essential services. The criteria for invocation should be set out in detail in the legislation and/or accompanying regulations, and should be published to provide certainty to stakeholders.
  - **Procedural Fairness:** The NCSC should be required to provide prior written notice to any entity that may be subject to denial of network access, setting out the grounds for the proposed action and affording the entity a reasonable opportunity to respond and, where appropriate, to remedy the alleged issue.
  - **Temporal and Substantive Limits:** Any denial of access should be strictly limited in duration and scope to what is necessary to address the specific threat identified. The criteria for review and lifting of the denial should be clearly articulated and made publicly available.
  - **Independent Oversight:** The exercise of this power should be subject to prior authorisation by the High Court or another independent body, mirroring the approach taken in respect of other intrusive powers under the Bill. In the absence of judicial oversight, a robust and independent appeal mechanism should be established to allow affected parties to challenge the decision.
  - **Application of Supervision and Enforcement Provisions:** The supervision and enforcement provisions set out in Part 8 of the Bill should be expressly extended to cover the exercise of this power, ensuring that appropriate checks and balances are in place and that the NCSC is held accountable for its actions.

3. Introduction of a Transition or Grace Period for Implementation

Current Position:

The Bill, as currently drafted, does not provide for a transition or grace period to allow stakeholders to prepare for the new regulatory requirements. I believe that such a grace period should be included for the following reasons:

Rationale and Recommendation:

- **Complexity and Impact of the New Regime:** The implementation of the NIS2 Directive and the associated national legislation will represent a fundamental shift in the regulatory landscape for cyber security in Ireland, comparable in scale and complexity to the

introduction of the GDPR. Both regulated entities and competent authorities will require time to adapt to the new requirements, develop internal policies and procedures, and ensure compliance.

- **Precedent and Best Practice:** The introduction of a transition period is consistent with best legislative practice and mirrors the approach taken in other major regulatory reforms, such as the GDPR, where a grace period was provided to facilitate orderly and effective implementation.
- **Recommendation:** A transition or grace period of not less than six months, and preferably up to twelve months, should be provided from the date of commencement of the Act. This will ensure that all stakeholders have adequate time to prepare for compliance and will reduce the risk of inadvertent breaches and associated enforcement action.

4. Additional Recommendations: Ensuring proportionality, transparency and avoiding unintended consequences

- **Safeguarding Critical Infrastructure:** The Bill should include 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.
- **Transparency and Accountability:** The NCSC 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. This will promote transparency, accountability, and public confidence in the operation of the new regime.
- **Stakeholder Engagement:** The Bill 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.

5. Conclusion

The National Cyber Security Bill represents a vital step forward in strengthening Ireland's cyber security posture and aligning national law with evolving EU standards. However, the powers conferred upon the NCSC, particularly under Head 3(1)(d), must be subject to clear limitations, objective criteria, and robust procedural safeguards to ensure that they are exercised in a manner that is proportionate, transparent, and consistent with the rule of law.

Under the NIS2 Directive, the country of origin is not more important than the implementation of active cyber protection requirements - if the government steers cyber resilience based on subjective criteria, the result is the opposite of what entire NIS2 directive aims to achieve.

The amendments proposed in this submission are designed to protect the interests of all stakeholders, safeguard critical infrastructure, and ensure the successful and sustainable implementation of the Bill. It is respectfully submitted that the Committee give careful consideration to these recommendations in the course of its pre-legislative scrutiny.

Finally, and more generally, we believe that while digital legislation is absolutely necessary to address the challenges and opportunities of the digital age, it must be carefully designed and implemented to avoid creating unnecessary burdens for businesses, be they large multinationals or SMEs, and hindering their ability to innovate and compete.