Opening Statement

Sean McElligott



Opening Statement of Sean McElligott before the Joint Committee on Justice, Home Affairs and Migration on certain aspects of the General Scheem of the National Cyber Security Bill 2024.

philiplee.ie

PHILIPLEE

DUBLIN | LONDON | NEW YORK

PHILIPLEE

Opening Statement of Sean McElligott before the Joint Committee on Justice, Home Affairs and Migration on certain aspects of the General Scheme of the National Cyber Security Bill 2024.

Chairperson, Members of the Committee, thank you for the opportunity to speak to you this evening.

My name is Sean McElligott, and I am a partner and head of the Technology Practice in Philip Lee LLP. Although I am a solicitor, my degree is in Electronic Engineering from UCD and before having an early life crisis and deciding to become a solicitor, I worked for 13 years in IT for, amongst others, Bank of Ireland Treasury and Motorola. The focus of my legal practice is therefore all things technology related.

The Heads of the General Scheme of the National Cyber Security Bill 2024 represent an important and timely step towards transposing the NIS2 Directive and placing the National Cyber Security Centre on a clear statutory footing. Stakeholders welcome the Bill's aims of strengthening resilience, improving incident response and deepening information sharing. The emerging EU implementing measures are already adding helpful specificity to concepts such as what constitutes a significant incident, and further ministerial guidance will support a coherent regime.

My observations, which have been set out more fulsomely across my previous submissions, are focused on the breadth and subjectivity of Head 3(1)(d). As drafted, it would allow the regulator to deny the use of network and information systems on grounds that include being detrimental to the interests of the State, being clandestine or deceptive, or involving a threat to any person, device or essential service. This power does not appear in the NIS2 Directive. Without objective criteria, clear thresholds and procedural safeguards, it risks arbitrary or inconsistent application, undermining legal certainty and proportionality. In short, a well-intentioned tool could become a blunt instrument with unforeseen consequences.

The practical risks are significant. Modern networks underpin hospitals, electricity grids and transport systems. 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. For example, locking hospital staff out of critical patient records, forcing blackouts when grid operators lose visibility and control, or halting railway traffic due to compromised signaling systems.

There is an internal inconsistency in safeguards across the Bill. The temporary deployment of sensors on communications networks under Head 9 is an intrusive but contained power that requires prior High Court authorisation. Yet the power to deny network access altogether could be exercised unilaterally, and the supervision and enforcement framework appears not to apply to it. If deploying a sensor calls for judicial scrutiny, the effective disconnection of an operator surely cannot require less.

For these reasons, I suggest that consideration should be given to either removing Head 3(1)(d) altogether or, if the Oireachtas considers that a denial power is indispensable for truly exceptional cases, it should be tightly constrained by law (at the very least, akin to the measures envisaged under Head 9). Any such measure should be:

- grounded in published, objective criteria tied to a clear, imminent and demonstrable threat;
- preceded by written notice with a fair opportunity to respond and remedy;
- strictly limited in scope and time with transparent review and lifting conditions;
- subject to prior independent authorisation or, failing that, to a robust, rapid appeal mechanism; and
- explicitly brought within the Bill's supervision and enforcement provisions.

© 2025 Philip Lee LLP. All rights reserved. Commercially sensitive and confidential.

In this way, explicit protections would ensure that actions taken under the Bill do not inadvertently disrupt essential services.

Two further points arise from my submissions.

Firstly, when addressing cybersecurity, priority must be on technical measures, standards, and internationally recognised certifications - non-technical or subjective factors should not influence cybersecurity outcomes. The NIS2 Directive's shift away from pure organisational and non-technical approaches, toward mandatory technical standards, is sensible and the NCSC's proposal to adopt the CyFun framework provides a structured, risk-based method for assessing maturity and preparing organisations for NIS2. Although CyFun does not guarantee compliance, it offers a credible basis for demonstrating technical capability. In addition, there is a growing consensus that ISO 27001 certification should be the foundation for achieving and evidencing NIS2 compliance. Its alignment with NIS2 has already led to formal recognition in several Member States, including Belgium, where ISO 27001 is explicitly accepted as proof that "essential" and "important" entities meet NIS2 cybersecurity requirements.

Secondly, a grace period of six to twelve months after commencement would support orderly implementation across both regulated entities and competent authorities, much as a transition period did for GDPR.

In conclusion, this is a strong Bill whose core architecture is widely supported. By removing, or decisively limiting the application of Head 3(1)(d), and by providing a measured transition and sustained transparency and engagement, the Committee can assist with the delivery of a regime that is both resilient and proportionate.

Thank you.
Sean McElligott.
Philip Lee LLP

© 2025 Philip Lee LLP. All rights reserved. Commercially sensitive and confidential.



PHILIPLEE

DUBLIN | LONDON | NEW YORK