Digital Rights Ireland and Irish Council for Civil Liberties

Opening Statement to Joint Committee on Justice, Home Affairs and Migration

General Scheme of the National Cyber Security Bill 2024

25 November 2025

Cathaoirleach and members of the Committee

We are very grateful to the Committee for the opportunity to discuss the General Scheme of the Bill with you.

When promoting cybersecurity it is important that we do not inadvertently create new security vulnerabilities or undermine fundamental rights and it is our concern that these Heads of Bill will have this effect.

The issues we raise are about parts of the Heads of Bill which are purely domestic innovations – that is, they are not part of the NIS2 Directive, have not gone through the European Union policy making and feedback process, and are not required to be transposed into Irish law. They must be considered separately and can be removed from the Bill without affecting transposition.

We would like to flag five aspects in particular.

Head 6 gives the NCSC power to scan networks for vulnerabilities in a way which is overbroad. It goes beyond NIS2, which envisages scanning of essential and important entities, and would permit scanning of small businesses, NGOs, or even homes. There is no justification in the Explanatory Note for this power and it is difficult to see why it is included.

Head 7 creates internet blocking powers for the NCSC which are extremely wide, unclear in their details, with very limited procedural safeguards. These powers should be reconsidered to build in greater procedural safeguards and effective independent oversight if they are to be compliant with EU law and the European Convention on Human Rights.

Head 8 provides for two entirely unprecedented powers. First, to scan and store the entirety of the network traffic in public sector bodies, including, for example, the contents of emails with sensitive health data, and the contents of emails to and from legal advisers. Second, to allow the NCSC to collect metadata about private communications on public networks such as mobile phone and home broadband providers and even messages sent via social network providers. This information could be stored by them for up to 18 months. Both powers can be used without the consent of any of the individuals affected. We say that this is clearly in breach of European Court of Justice caselaw prohibiting the bulk collection of the contents of communications and metadata about communications, particularly as Head 11 would allow this information to be shared with the Garda Síochána.

Head 9 raises the same concerns about mass collection of communications data, exacerbated by the fact that it would create a *compulsory* power by which the NCSC could compel communications providers, services such as WhatsApp and iMessage, and data centre operators to install surveillance devices on their networks. This would permit collection of data on the telephone and internet use of the whole population, on national security grounds, without any requirement of proportionality. Notably, 'national security' is not defined anywhere in the Heads of Bill.

Finally, Head 10 deals with the NCSC's power to process personal data for new reasons, beyond those for which the information was collected. It creates a largely open-ended power to do so, including for any national security reasons. This compounds the earlier concerns about bulk collection of communications content and metadata, as it would permit the NCSC to handle that data for new and unspecified national security purposes, beyond the reasons for which the data was originally collected.

Thank you for your time and we would be very happy to address any points you may have.

Dr. TJ McIntyre
Chair, Digital Rights Ireland CLG