Chair, Committee Members,

Thank you for the invitation to meet with you today to discuss the General Scheme of the National Cyber Security Bill and, also, your previous invite to make submissions is respect of this Bill, which was very much appreciated.

As a result of our responsibility to investigate such crimes after they have occurred; An Garda Síochána get a very clear view of the harm caused by cybercrime and the personal impacts that result. Unfortunately, many result from deficiencies in cyber hygiene practices, even at the most basic level of employee awareness concerning phishing or social engineering.

Having regard to the above, the beneficial impacts of the Network and Information Security Directive and its transposition into Irish law by the National Cyber Security Bill 2024 are most welcome as mechanisms to create a more secure cyber eco-system in this jurisdiction. The Garda National Cyber Crime Bureau and the National Cyber Security Centre maintain a productive working relationship and both agencies are frequent collaborators and support each other's respective roles, particularly in the area of cybercrime prevention.

By way of general overview, the cybercrime economy is frequently cited as being the fastest growing in the world and by the end of 2025, it is estimated that this figure will be just over €9 trillion, up from an estimate of approximately €5.5 trillion in 2020. There is little doubt that the cybercrime economy is now an economy of scale and one that is generating immense wealth for those who benefit from it, while causing immense harm to victims.

Despite representing a smaller proportion of the cybercrime economy, in terms of financial output, it is my respectful assertion that cyber dependent crimes, which are offences that can only be committed using a computer, represent the greatest threat of societal level disruptions. Within this category, ransomware, which is a type of malware that encrypts the victim's personal data until a ransom is paid, represents the most significant threat.

In terms of supporting this assertion, I point to the impacts of the largest such attack in Ireland; on the Health Services Executive in 2021, and more recently; disruption to flights in a number of countries, including Ireland, due to an attack on an airline services provider; to operations of a major retailer in Ireland and the UK and the negative impact on the UK's recent GDP figure, attributed to ransomware disrupting the operations of a vehicle manufacturer. These examples display the disruptive impacts and potential for cross-societal harm created by the perpetrators of cyber dependent crime.

In addition, the dynamic in respect of those perpetrating cyber dependent crimes is becoming increasingly complex. Criminal groupings have become highly organised employing specialists and sourcing ransomware toolkits as a service. There is evidence of nation state involvement in cyber-criminality. Finally, there is access to ever increasing computational power, network capacity and new technologies, such as artificial intelligence; all of which extend reach and create enhanced capacity to deceive.

The net outcome is that Cyber-criminality, in all its forms, represents a clear and present danger to the normal functioning of the many services we, as a society, have come to rely upon. It is also very apparent that there is an absolute necessity for all those who operate within this eco-system, particularly as service providers, to maintain a proactive, resilient, cyber security posture to support its effective operation. In this context, this Bill is viewed as a very important legislative development.