Internet Policy Division – Consultation
Department of Communications, Climate Action & Environment
29-31 Adelaide Road
Dublin
D02 X285

American Chamber of Commerce Ireland
6 Wilton Place, Dublin 2, Ireland
T: +353 1 661 6201
F: +353 1 661 6217
E: Info@amcham.ie
www.amcham.ie

1st May 2019

Re: National Cyber Security Strategy Public Consultation

Dear Richard,

The American Chamber of Commerce Ireland greatly welcomes the development of the next National Cyber Security Strategy (the 'Strategy') for Ireland. The American Chamber's 2019 Cyber Security Position Paper (which you will also find attached) demonstrates how Ireland is well positioned to leverage the presence of many global and indigenous companies to show leadership as the 'Strongest Link in the Chain' when it comes to cyber security.

The American Chamber views this strategy in the context of its vision for Ireland to be **'an inclusive location-of-choice for talent and innovation with global impact'.** Given that the competition for investment internationally is intensifying in the face of changing global trade policy and political uncertainty, the American Chamber believes that Ireland must focus on the domains it can control in the face of geopolitical, economic and social developments to sustain competitiveness for inward investment. Having an international reputation for robust and resilient cyber security policies and systematic practises, is one such strategically important domain. That reputation is a whole of Government responsibility to protect public services, critical national infrastructure and the economy and not limited to Government Departments and Agencies with explicit front-line responsivity for IT, communications and cyber security.

Cyber security or cyber-safety is an ever-present, mercurial challenge for all organisations – from large global companies to SMEs and has impacts far beyond just the digital leadership of 'tech' based businesses. From healthcare to fashion, banking to food, travel to communications, public sector, community and private enterprise – all sectors face cyber security threats across supply and delivery networks. Further, as increased connectivity is driven by advances in cyber-physical and IoT worlds, and as the Industry 4.0 revolution takes hold, the demands on protecting global supply chains is highly significant.

The American Chamber is strongly of the view that the development of the next National Cyber Security Strategy is a critically important step in achieving the aim for Ireland to be a global cyber security leader. Having consulted with a cross-sectoral and geographically spread representative group of member companies the **American Chamber's Vision for the next Strategy is to see Ireland recognised as having a robust and resilient cyber security policy and systematic practises under the leadership of an established and esteemed National Cyber Security Centre**. In doing so, Ireland should take a risk-based approach to cyber security regulation to support efficient approaches to meet compliance obligations.

That Vision emphasises the following priorities for the next national Strategy:

- **Cyber Security as a recognised Competitiveness Issue for Inward Investment**
  Ireland operates in an globally connected policy and cyber security environment. As well as an EU framework, digital connectivity between Europe and North America represent some of the largest data flows in the globe with 8 of the world's most connected countries globally being in Europe[i].

Companies doing business globally want to ensure their assets are protected in an environment which is secure and resilient. The extent to which a country invests in and prioritises cyber security and has a reputation for high standards of cyber-security practices can determine critical FDI decisions.

- **Sustained Investment for Ireland's National Cyber Security Centre (NCSC)**
  The American Chamber has a long-held positive position regarding the investing in the capabilities and reputation of competent authorities in Ireland, such as the Data Protection Commission (DPC). It is crucial that the NCSC receives significant and sustained support to enable the recruitment of skilled and experienced staff, to deliver on its mandate and to increase its public profile. Such competent authorities need to operate in an environment that reflects their institutional importance, is attractive to talent and enables appropriate levels of public-private interactivity. Government ambition for the appropriate scaling of the NCSC is required, with reference to like-jurisdictions (e.g. Denmark or Sweden), to deliver on its mandate. Ireland should ensure that the roles and remits of institutions working on cyber (such as the NCSC and DPC) are aligned, clear and transparent to avoid unnecessary compliance burdens and/or duplication of effort.

- **Addressing the Skills Gap**
  Fostering, attracting and retaining talent in the public and private sectors – with both technical expertise and soft skills – is crucial to creating a robust cyber security environment. The American Chamber recommends that these cyber-safety/health skills be embedded at the earliest stages of education in Ireland. There is an opportunity to develop and crystallise an attractive future for those seeking a career in cyber-security/safety – a pathway with diverse opportunities for technical, strategic, regulatory and commercial excellence. The existing workforce should also be tapped into by developing opportunities and programmes to facilitate skills conversion, upskilling and leadership development of staff.

- **Public Private Dialogue**
  Public and private sectors working together is essential to meeting cyber security challenges. The establishment of a Centre of Excellence for Cyber Security would provide an opportunity for the public sector, academia and the private sector to engage in dialogue, exchange ideas and explore topics, solutions and policies to meet the dynamics of an every-changing cyber environment.

The American Chamber welcomes the opportunity to input into the development of the next National Cyber Security Strategy. Indeed, the consultative approach undertaken by the Department of Communications, Climate Action and Environment throughout this process is appreciated. The American Chamber is confident that by building on the experience and data accumulated since the last national cyber security strategy, and encompassing the priorities listed above, great strides will be made in applying Ireland's digital leadership credentials to the global cyber security stage.

Please don't hesitate to contact the American Chamber should you wish to discuss the above priorities in greater detail.

Yours sincerely,

Brian Cotter
Advocacy and Public Affairs Director

[i] The Transatlantic Digital Economy 2018, Centre of Transatlantic Relations, John Hopkins University WA DC