Mr Pat Rabbitte TD
Minister for Communications, Energy and Natural Resources
Department of Communications, Energy and Natural Resources
29-31 Adelaide Road
Dublin 2

3rd March 2014

Dear Minister,

The American Chamber of Commerce Ireland supports the European Commission proposal to introduce a Network and Information Security (NIS) Directive to underpin the EU's broader cybersecurity agenda. The ambition of the draft Directive to ensure that all Member States are adequately equipped to facilitate information sharing and cooperation to further that agenda is very welcome. It is also welcome to note the objective of the Directive to develop national NIS capabilities, including National Computer Emergency Response Teams (CERTs) and cybersecurity strategies. These capabilities are vital to protect every business in Ireland.

The Chamber supports the Government's objective of making Ireland the leading tech-hub in the EU. There have been many welcome advances along that path; however, it is vital that this objective is not undermined by any lack of preparedness to deal with security threats to critical infrastructure. Ireland is home to some of the world's largest technology, utilities and financial services companies. These organisations provide, or support, essential critical infrastructure in this State. The NIS Directive, if it reflects industry concerns, will be a crucial framework within which that security can be protected.

It is essential for Ireland with its large and growing high-tech sectors to aim for world class standards as a means to attract further investment. Effective information and security practices must be in place in order to ensure continued security and to foster further inward investment in these growing sectors. When considered at a sector level, Ireland is the No. 1 location worldwide for US FDI in the chemicals sector, which includes pharmaceuticals, and second worldwide in the information sector. Increasingly we are attracting firms that specialise in cybersecurity and preparedness. Continued possession of these enviable commercial strengths will be enhanced by a reassurance to investors of Ireland's capability to guarantee the security of its critical infrastructure. At a minimum this will require effective information and network security practices.

While the draft Directive is a welcome step for the EU there are a number of areas in which it could be improved during the impending legislative process. We outline our suggestions for change below.

American Chamber of Commerce Ireland
6 Wilton Place, Dublin 2, Ireland
Tel: +353 1 661 6201
Fax: +353 1 661 6217
Email: info@amcham.ie
www.amcham.ie

Scope of the Directive

The overarching aim of the Directive is to improve the network and information security of companies operating critical national infrastructure. While we support this objective, we believe the scope of the Directive is too broad and should be refined. If adopted as drafted by the Commission the proposals would apply to companies that have no impact on critical infrastructure. The inclusion of such an all-encompassing term as 'information society services' in the Directive would encompass companies that have no relevance to the core functioning of society.

The online world has certainly become part of our citizens' and public and private organisations' everyday life. Companies and nation states are facing increasing levels of threat posed by 'hacktivists', criminal networks and in some cases state sponsored actors. Measures need to be taken to ensure that companies take the necessary steps to mitigate the risks faced to their systems and networks. However this does not mean that all companies that provide 'information society services' should be subject to the obligations set out in the Directive. The indiscriminate inclusion of a whole host of information society services irrespective of their actual criticality or relevance to critical infrastructure is unjustified. What are vital to protect are the indispensable services, as opposed to the 'nice to have' services. If social networking sites, or cloud based e-commerce platforms went down, then society would still function. Companies would no doubt have some disgruntled customers, but these customers could not argue that they were considerably inconvenienced in the same way as if they did not have access to electricity or water. This is a key distinction: what is vital to the full functioning of society as distinct from what is not.

The Committee on the Internal Market and Consumer Protection (IMCO) of the European Parliament recently voted to remove references to information society services from the draft Directive. We support the Committee's decision and submit that no future iterations of the Directive should reintroduce this aspect.

Incident report and information sharing requirements

Information sharing forms a major part of the proposed Directive. Article 8 proposes the establishment of a cooperation network across member states, which would share information through a secure information system, as proposed by Article 9. Article 10 requires competent authorities to provide early warnings on risks and incidents and Article 14 requires market operators to notify competent authorities of security incidents.

Information sharing should form an essential aspect of any strategy to address the security of key elements of the critical infrastructure; it can be a crucial tool in helping companies to protect systems, networks and customer data, as well as IP from theft or manipulation.

Information sharing is an effective way of gaining intelligence and wider situational awareness of the threat landscape and can form an important part of a company's or nation state's approach to risk management. In addition, incident reporting can be effective in improving risk management and security if part of a process for preventing and remediating breaches. However, incident reporting should not be a goal in itself, nor a sanction on the victim, or a bureaucratic burden, and it should not put an organisation's reputation at risk.

There are a number of existing information sharing initiatives in operation across Europe and the Commission should seek to build on these existing mechanisms. Information should be perceived as a mutual benefit to both the public and private sectors, and models are most effective if they are built on trust, with a shared vision and objectives. Information sharing and reporting should not be conducted one way – operators should also receive intelligence that will enable them to improve their infrastructure. This is all the more important because, as the draft Directive explicitly recognises, much of the critical infrastructure to be protected is run by those operators.

Information classification

It is important to recognise that the information shared will be sensitive by its very nature, and as such ensuring the security of the information shared is crucial. A safe and secure reporting system should be in place to ensure the confidentiality, protection and secure handling of the information. A secure information sharing environment will provide industry with the assurance that any information shared will be managed according to its operational and legal sensitivity. The American Chamber of Commerce welcome the recognition of the IMCO Committee of the need for information to be classified and protected according to its sensitivity, specifically its inclusion in the proposed amendment to Recital 38 of the Directive.

Industry safeguards

It is crucial that companies should not be penalised for sharing information; and the Directive should not expose companies to litigation or regulatory sanctions. American Chamber members have voiced concerns that the drafting of Article 17 could be interpreted as meaning that operators will face automatic sanctions in case of a breach. This would prove a very clear disincentive to report any breach, which would clearly run counter to the purpose of the incident reporting scheme envisaged by the European Commission. A sanctions based reporting scheme would penalise companies with effective cyber security procedures in place, as they will be more equipped to detect a breach, as opposed to companies that do not have effective breach strategies or capabilities. On top of discouraging information sharing in the first place, this type of scheme would also effectively reward companies with lower levels of network and information security capabilities. The combination of these two aspects would clearly result in a double perverse unintended consequence.

Competent authorities should not further share, let alone publicly disclose the information without at least informing the source company in question, as this could potentially damage the company's security, safety or reputation and effectively penalise them as a result. The information shared should not be made public without the explicit consent of the originator of the information (i.e. the market operator that experienced the breach). Experience has shown on many occasions that premature or ill-considered public disclosure of breaches can weaken rather than strengthen cybersecurity, whereas information sharing mechanisms can be successful and rewarding without a public disclosure component. In fact, in many cases, public disclosure might be perceived by participants as a risk, and therefore a disincentive that inhibits rather than fosters information sharing.

Standards and technical capabilities

Article 16 proposes that Members States should encourage the use of standards and/or specifications relevant to network and information security. Effective implementation of security management standards can help businesses understand the risks to systems, networks and information, and help organisations put in place the necessary controls to protect themselves, thereby minimising the risk of attacks or accidental incidents.

Network and information security standards provide industry with effective means of understanding the measures that they need to undertake to enhance an organisation's policies and processes and to embed security within their operational structure. Standards that are developed and/or promoted in Europe should be consistent with global developments. As cyberspace transcends geographic borders, the Commission and Member States should not develop EU-centric standards, and should instead focus on promoting existing industry-led, globally recognised standards. A regime based on compliance/mandatory requirements can undermine the notion of cooperation and trust that already exists within Member States.

Formal adherence to technical standards could be counter-productive. Such standards cannot keep pace with advances in technology, or the threat landscape, and can quickly become obsolete. Moreover, over specifying the standards that organisations should comply with does not provide the flexibility necessary to mitigate the threats organisations are faced with, and can lead to a company taking a 'tick box' approach to compliance that creates a false sense of security. Companies are better placed to understand their risk profile and should be given the flexibility to adopt the standards, processes and technologies that most suit their organisation.

Member states should encourage the adoption of standards and, where necessary, provide guidance on what can be seen as a complex landscape. This is precisely the approach that the US has taken with the Framework for Improving Critical Infrastructure Cybersecurity, which was launched in February 2014. The Framework was developed collaboratively with industry and consists of guidelines, and practices to promote the protection of critical infrastructure, and importantly takes a flexible and voluntary approach. It enables organisations to utilise standards and guidance that suit their business and security posture.

We welcome the amendments proposed by the IMCO Committee, which in contrast to the Commission text, reference international standards and not just European standards. In addition, the IMCO amendments recognise the importance of giving suppliers the flexibility to decide the most appropriate compliance regime by clearly stating that Member States should not prescribe the use of particular technology.

Harmonisation of requirements

The Chamber appreciates the rationale for proposing the minimum harmonisation requirement as Member States, and the operators working within them, will have varying levels of network and information security. However the minimum harmonisation principle may lead to a fragmented approach across the EU, especially with regard to incident reporting, and will place an added burden on cross-border operators who will have different legal obligations across the EU. In addition, given

the global nature of NIS incidents they can in many circumstances cross borders and jurisdictions, and therefore a harmonised approach within the EU is essential.

If the minimum harmonisation requirement is maintained then it needs to be balanced with clear rules on jurisdiction and applicable law for market operators who do business across several Member States.

Coordination with the General Data Protection Regulation

As highlighted above, the information shared by operators may be sensitive by its very nature. At the same time, parts of it may also qualify as personal data under data protection law. Therefore it is important that the Directive clearly sets out the articulation between the NIS legislation and any relevant privacy rules, such as those of the draft General Data Protection Regulation. Tensions may form between the implementation of the NIS Directive and the requirements of Data Protection law within Member States, and because of that the Directive should clearly distinguish the rules applicable to data processing, information sharing and incident reporting under the two regimes, as well as the roles and responsibilities of the competent NIS authorities, and respectively the data protection authorities.

Minister, the American Chamber is keen to see a robust and usable framework developed throughout the EU for network and information security. Security is an increasingly valued commodity for business and consumers. The competitiveness of EU based businesses will be boosted by a clear and workable approach to security. We believe that there is now an excellent opportunity to ensure that such an approach is introduced and that this is vital for the continued success of Ireland's attraction of high tech multinationals to Ireland.

Yours sincerely,

Brian Cotter
Public Affairs Director

cc: Mr Mark Griffin, Secretary General, Department of Communications, Energy and Natural Resources