American Chamber of Commerce Ireland

Submission to the Consultation on the Network and Information Security Directive

Department of Communications, Climate Action & Environment

December 2016

Introduction

The American Chamber of Commerce Ireland has engaged extensively with its member companies on the various aspects of implementation of the Network and Information Security Directive (NIS).

The key priority for the Chamber is that Ireland remains a global location of choice for US foreign direct investment (FDI) into Europe, and by doing so we retain and attract further investment and jobs.

The American Chamber of Commerce Ireland is committed to working with Government to ensure that the policies Ireland adopts are best-in-class and assist in fostering growth and innovation.

The Chamber has reflected this stance in its response to the thirteen questions posed by the Department of Communications, Climate Action & Environment on the implementation of the NIS Directive.

Question A: Are the means outlined the most appropriate framework for the State to deliver on the requirements of the Directive (i.e. NCSC as an Office of the DCCAE)?

The American Chamber of Commerce Ireland believes that the framework outlined to establish the National Cyber Security Centre (NCSC) as an office of the Department is the correct approach.

Question B: Is combining regulatory and operational functions i.e. the National Competent Authority and national CSIRT within an existing civil service structure (i.e. a Government Department) appropriate?

- In general, we support the combination of regulatory and operational functions.
- This would need to ensure that the appropriate separation of duties creates a system of checks and balances.
- To ensure efficiency and to prevent a duplication of regulation, there should be absolute clarity about the respective responsibilities and objectives of the different component parts. Digital Service Providers (DSPs) and Operators of Essential Services (OESs) should have clarity on who their relevant points of contact are, and with what competencies.
- Such a combination seems reasonable, as part of a holistic Government response that takes into account the need to have a flexible, innovative, yet safe and secure digital infrastructure, that supports Ireland's globally competitive digital economy.
- The American Chamber of Commerce Ireland would particularly urge that there is co-ordination with the Irish Data Protection Commission, to ensure harmonisation and

no conflict or duplication with the national implementation of the General Data Protection Directive.

Question C: How should the obligations for a national network and information security strategy be met?

- Network and Information Security crosses national borders and involves private and public stakeholders. It is critical that the National Competent Authority takes both these points into account when seeking to meet the obligations of the information security strategy. This can be achieved by:
  - Establishing a regular exchange of information and security strategy with private companies who are OESs or DSPs, including on the implementation of the NIS Directive.
  - Ensuring that the national implementation process reflects existing international best practice guidance, that is process-orientated and risk-based, taking cognisance of existing international standards.
  - Establishing a regular exchange of information and strategy with other National Competent Authorities. Given that the Irish National Competent Authority is responsible for a significant number of global companies, it should seek to ensure consistent practices are implemented across the EU - one of the clear objectives of the Digital Single Market. Industry could assist in identifying what other member states' National Competent Authorities, Ireland could benchmark itself against.
- To support the effective implementation in a fully functioning digital economy, the new National Cyber Security Centre and the National Cyber Security Strategy should be adequately funded and resourced, including with the relevant expertise.
- The national NIS strategy must create an environment that promotes a culture of risk management among OESs and DSPs, based on risk assessment and the implementation of security measures appropriate and proportionate to the risks faced. It must also facilitate appropriate trust-based information exchange and must not become a static or "box-checking" compliance exercise. As the nature of cybersecurity threats evolves rapidly, any successful NIS strategy must remain agile and provide for ongoing dialogue among stakeholders.

Question D: Given the anticipated need for sector specific expertise, what approach should Ireland take in regard to engagement with these EU co-operation and co-ordination arrangements?

- Ireland should participate fully in the Cooperation Group and in the CSIRTs Network envisaged in the NIS Directive, in order to benefit from the experience of other Member States, and to represent Ireland's interests. It is absolutely crucial that the National Competent Authority engages regularly with the EU Agency for Network and Information Security (ENISA). As the competent EU agency, ENISA's structure, area of competence and guidance should act as a model for the National Competent Authority. This will also assist in the harmonisation of National Competent Authorities' approach.
- The Chamber understands that the NCSC will act as the relevant national competent authority for Digital Service Providers with their European headquarters based in Ireland, even in respect of incidents arising from their services in other EU Member States. There are therefore particular responsibilities for the Irish National Competent Authority in order to cooperate with other national competent authorities. Indeed, Ireland should show leadership in this regard.
- DSPs may have network and information systems across many member states. Clarity around jurisdiction and oversight will be important factors in ensuring that the implementation of the NIS Directive enhances the functioning of the Digital Single Market.
- The consistency in the information / cyber security reporting arrangements between the National Competent Authorities (in each EU member state) and ENISA will be key to the efficiency and effectiveness of the NIS throughout Europe.
- Adequate funding and resourcing of the National Competent Authority will be necessary to ensure effective engagement is achieved.

Question E: In the case of the CSIRT-Network which involves voluntary operational co-operation, should information about incidents involving Ireland be shared with other Member State CSIRTs participating in this network?

- It is important that the Government establishes a clear governance process that includes rules on appropriate management of the data shared, from its creation and release to its use and destruction.
- Ireland should work with other Member States to create lines of communication among the various authorities that enable a single notification of incidents, without prejudice to business confidentiality.
- The Chamber supports the development of EU wide guidance from ENISA on Security Incident Reporting. This consistency will assist in information sharing, providing clarity on what should be legitimately shared and in what circumstances. Consideration should be given whether such sharing increases the impact of such an event, including through impact on the economy or, through knowledge of the event, of similar events taking place.

Question F: Could such information being shared include personal data, such as IP addresses, for the public interest purpose of network and information security?

- Sharing of such information should only be permitted where it is would enhance security and it is justified by public interest.
- An EU wide protocol would need to be clearly defined and agreed.
- A gap analysis with GDPR is necessary in order to ensure that information which is shared is consistent with the General Data Protection Regulation. This will assist in the definition of common standards, the prevention of duplication of effort and reporting including with other EU member states), and the reduction of risk, through preventing the unnecessary sharing of any personal data.
- Regulatory clarity between all existing and new sets of regulation is critical.

Question G: How should the State go about the process of identifying and designating 'Operators of Essential Services'? In particular, how can the business interests of candidates be reconciled with security and reporting obligations?

- Clear guidance and definitions needs to be provided to identify OESs, with a clear rationale for their designation.
- The Chamber is of the view that once the State publicises the requirement and the relevant definitions, it is in the interest of OESs to self-identify.
- The establishment of an effective stakeholder consultation mechanism and the sharing of experience from the Cooperation Group and other Member States will be helpful in ensuring a coherent and risk-based approach to designating OESs, consistent with the approach set out in the NIS Directive.

Question H: What should the security requirements of Operators of Essential Services amount to, beyond risk management matters? How can the NCSC be assured that appropriate risk management measures are in place in each operator of essential service in accordance with Article 14(1) of the Directive?

- As Article 14(1) implicitly recognises, when it refers to *"Having regard to the state of the art…",* the specific security measures appropriate to an OES will change over time as the nature of cybersecurity threats and of risk management techniques and technologies evolve.
- The NCSC should not mandate specific technologies, but rather refer to minimum standards, such as those in the NIST cyber security framework or relevant ISO or equivalent standards.

Question I: What type of guidance would be appropriate for Operators of Essential Services in determining the significance of an incident for reporting? How should thresholds for mandatory reporting of incidents be developed?

- The NCSC should develop guidance on incident reporting in consultation with stakeholders, including clear definitions of the key terms.
- Clarity in the division of reporting responsibilities where an incident involves personal data and therefore requires reporting to the Data Protection Commissioner should also be ensured.
- If reporting thresholds are set too low there is a risk of the national CSIRT being overwhelmed with insignificant incident reports, thereby wasting scarce resources and defeating the overall objective of the NIS Directive.
- While specifically-defined thresholds may appear attractive in terms of providing clarity, any fixed threshold is essentially arbitrary, and it may be more effective to allow OESs some latitude in determining whether a given incident should be reported, by reference to its impact.
- Guidance in the form of hypothetical and real examples would be helpful, and would be a useful topic for the Cooperation Group to address. The guidance should also set out how the information on a reported incident will be used, and processed further.

Question J: Should the identity of designated Operators of Essential Services in the State be a matter of public record?

- The Chamber is of the view that publicly available information should avoid listing actual infrastructures, either by only naming the sectors or by providing only head office information.
- Publishing a national list of OESs would in itself increase the national security risk.

Question K: Should the Department establish a stakeholder group of digital service provider representatives to highlight implications and influence developments with the European Commission's process to finalising implementing acts on security requirements and notification obligations for Digital Service Providers?

- The American Chamber of Commerce Ireland is firmly of the view that in order to achieve the objectives of the NIS Directive, strong cooperation among all the parties is essential.
- A stakeholder group would provide a valuable mechanism for consultation, sharing of experience and ongoing improvement.

Question L: When should the NCSC be ready to fulfil the National Competent Authority in respect of Digital Service Providers, noting the need for cross-border co-operation i.e. after the implementing acts are finalised in August 2017 or by the transposition deadline of May 2018?

- The American Chamber of Commerce Ireland recommends that, given the work required to identify, codify and fulfill national obligations of the NIS with in respect of DSPs, as well as create processes and structures, Irish authorities should aim to have an effective and appropriately-resourced National Competent Authority fully operational by the transposition deadline of May 2018.
- A realistic timeline such as this will also allow Ireland to assess and benefit from the early experiences of other Member States.

Question M: Having regard to the light touch approach for Digital Service Providers, referenced in recital 60 of the Directive, how should the implementation and enforcement measures of the NCSC differ from those applied to Operators of Essential Services?

- Given that the degree of economic and societal risk for an incident affecting an OES would be substantially higher than for an incident involving a DSP, implementation and enforcement measures in respect of DSPs should be less stringent than those for OESs. The NIS Directive explicitly recognises this principle, for example in Recitals 49 and 60.
- Since the Directive explicitly recognises that DSPs should have appropriately lighter obligations than OESs, it should be clear that DSPs are not under an obligation to report incidents to the competent authority unless the availability/continuity of the service is significantly impacted. Moreover, when an OES relies on a third-party DSP for the provision of an essential service, incidents reported to the competent authority by the OES should be limited to those involving significant impact on the continuity of the essential service (Art. 16.5 of the NIS Directive).
- This 'significant impact' needs to be clearly defined.
- The Directive does not refer to the integrity or the confidentiality of the essential service as notification parameters, so broadening the scope of DSP obligations by requiring that DSPs report incidents in cases where confidentiality and integrity were affected, would therefore not be consistent with the Directive.
- A DSP incident should be reportable only when it is a confirmed event that results in an actual adverse effect on the continuity or availability of a digital service, and there is a substantial impact on economic or societal activities. Clear parameters need to be set in this regard.

- Security baselines for DSPs should be risk-based and outcome-focused and take into account international best practices such as the NIST Cybersecurity Framework.
- Maintaining the light touch across Member States will ensure harmonisation in the implementation of the Directive.
- Implementation should recognise existing international and industry standards on incident reporting and cyber security standards, including the implementation of security measures appropriate to each company, on a risk based model.
- An unnecessarily heavy-handed approach will have an impact on the functioning of the Digital Single Market. This impact could be twofold:
    1. Prevent DSPs effectively operating across the EU;
    2. Impact on innovation and flexibility of companies who are obliged to concede to burdensome regulation.

The Directive underlines that DSPs are subject to reactive ex-post supervision and hence competent authorities do not have any general obligation to supervise DSPs and should only take action when provided with evidence. These provisions should be honoured when implementing the Directive.

Concluding Remarks

The American Chamber of Commerce Ireland welcomes the opportunity to input into shaping the implementation of the NIS Directive in Ireland. Ongoing consultation and cooperation is essential as we work towards the collective aim of making the Irish Internet space a secure place for all, adopting best-in-class security procedures.