AMERICAN CHAMBER of COMMERCE IRELAND

Submission to the consultation on the proposed revision to the Directive on Security of Network and Information Systems (NIS Directive)

19 March 2021

Introduction

The American Chamber of Commerce Ireland (henceforth 'the American Chamber') is the leadership voice of US business in Ireland. Our mission is to strengthen the transatlantic business community through advocacy and networking with purpose. American Chamber membership includes US companies operating from Ireland, Irish companies expanding in the US and organisations with strong bilateral links between Ireland and the US.

The American Chamber strongly welcomes the opportunity to submit to the Department's public consultation on the proposed revision to the Directive on Security of Network and Information Systems (hereafter 'NISD2') and in particular the opportunity to highlight how the current proposed revision of NISD2 would impact our on our members. As the digital transformation of society intensifies, particular in the wake of the pandemic, and as the revised version of NISD2 proposes to cover more sectors and services considered to be of vital importance to the European single market, the American Chamber underlines that it is vitally important that the National Cyber Security Centre (NCSC) continues to be funded and resourced to reflect the level of responsibility

Executive Summary

Overall, the American Chamber welcomes the expanded scope of NISD2 however there a key issues outlined below, and further on in detail, that need to be taken into account, including:

- **Regulatory consistency and harmonization** is required between NISD2 and other EU legislation including DORA[1], the EECC[2] and GDPR[3]
- The proposed **timeframe for reporting initial incidents is too short** of a timescale (24 hours) and should be aligned with GDPR (72 hours)
- The **obligation to report potential threats or 'near misses' is problematic** and should not be included
- Vulnerability reporting rules should be amended to clarify for entities that there is **no obligation to report vulnerabilities that have not yet been patched**
- As it stands the **enforcement provisions and fines outlined are disproportionate** and do not offer the best incentives to achieve a productive and trustworthy collaboration between entities and authorities
- **Cybersecurity certification should remain voluntary** and not be made mandatory as this is not in line with the intention of the EU Cybersecurity Act

[1] The Digital Operational Resilience Act (DORA)
[2] The European Electronic Communications Code (EECC)
[3] The General Data Protection Regulation (GDPR) 2016/679

- **It should be clarified as to why mandatory IT security training is necessary for members of management bodies**, and whether reports by CISOs or IT security personal would be equally sufficient to provide members of management bodies with in-depth information
- **Security requirements and risk management measures need to be less prescriptive** and allow the organisation to adopt a risk based approach.

Regulatory consistency and harmonization

The American Chamber notes that it is important to ensure that entities covered under NISD2 have legal certainty of when NISD2 applies and when other EU legislation is applicable. Regulatory consistency is key, and ensuring that there is harmonization between NISD2, DORA, the EECC, and GDPR. As it stands, these regulations and directives all have related but inconsistent reporting requirements (e.g., timeframes, level of information/detail, and potential non-compliance penalties). The focus should be on containment and recovery of the incident. **Reporting requirements need to be streamlined to avoid overlapping and/or conflicting obligations**.

For example, while the American Chamber welcomes that some digital service providers who provide services in different member states fall under the jurisdiction of their main headquarter in the EU it is not clear why this provision is not extended to all entities under the "digital infrastructure" section in Annex I who also typically operate across borders. Applying Art. 24(1) to all digital infrastructure services would increase regulatory consistency across the EU and increase harmonisation.

In order to support Member States in strengthening their respective capabilities and competences, and improve (cyber)security and resilience, NIS2 should ensure that there is no duplicate reporting required amongst all cyber related legislative proposals, while at the same time acknowledging the attributes of different sectors.

Alignment with the EECC (European Electronic Communications Code)

The American Chamber highlights that alignment between the European Electronic Communications Codes (EECC)'s security provisions and the NISD2 is critical for providers of electronic communications services and networks ("ECS/ECN").

Recital 49 of the NISD2 states that EU Member States should continue to enforce certain paragraphs (40.1, 40.2) of the EECC's national transposition laws for the purposes of the NISD2, with the result that telecom services may fall under the national transposition of the EECC for some provisions and the NISD2 for others, creating legal complexity and potential fragmentation across Member States.

The intention of this recital is welcomed, in that it aims to ensure some level of continuity for ECS/ECN providers, notably for the parameters around incident reporting where those providers who already

have legacy systems in place can continue to use them, and remain subject to similar security provisions under the EECC (and the earlier Framework Directives).

To ensure that all ESC/ECN providers captured within NISD2 are subject to the same oversight, reporting requirements and security measures, and to avoid unnecessary duplication of obligations, the **American Chamber recommends that only one proportionate regime is applicable to ECS/ECN providers, and that the security provisions within the EECC should be repealed to allow NISD2 to take precedence, while retaining Recital 49 to avoid unnecessary burden for ECS/ECN providers who already have relevant and similar security processes in place. NISD2 should also reinforce the use of the one stop mechanism and that ECS would be subject to NISD2 in a single jurisdiction and not in each jurisdiction in which they provide services in.**

If this cannot happen, and a mixed approach is taken, then it is important that complexity and fragmentation is kept to a minimum , for example, through the development of EU-level guidelines or similar. ECS/ECN providers require legal certainty and simplicity as regards the enforcement of certain security provisions under the EECC and separate provisions under the NISD2. Provisions in either text should not contradict each other and should not result in duplication of responsibilities.

Alignment with DORA (Digital Operation Resilience Act)

The American Chamber recommends introducing a clear hierarchy between NISD2 and DORA to avoid fragmentation and conflicting obligations for entities that are captured within both. Where entities are subject to both, DORA should take precedence.

The proposed DORA Regulation is envisaged to function as *lex specialis* (the more specific of those laws will override the general law) to the current NIS Directive regarding ICT risk management requirements and cyber incident reporting. Therefore, it was intended that the relevant NIS provisions will no longer be in effect for financial entities included in the scope of both the NIS Directive and the proposed DORA regulation. Since the drafting of DORA, the NISD2 refresh has commenced and it has not yet been confirmed whether the same will apply when NISD2 comes into effect.

In particular, there is a high risk of conflicting recommendations coming out of the two separate supervisory/oversight processes from the different regulators if no single mechanism for the competent authorities to share information and coordinate their practices is established. In particular:

- On definitions, NISD2 defines "incident", while DORA defines "ICT-related incident". The American Chamber recommends that NISD2 should align with the DORA definition.
- On reporting, DORA is concerned with "major ICT-related incidents" while NISD2 with "incidents that are significant". This requires better alignment.
- On timeframes, there are inconsistencies in relation to the point at which the timeframes for incident notification begin. It would be preferable if timeframes for initial notifications and status updates were consistent and take into account that some entities may have requirements to

report under both (whether directly or indirectly through contractual requirements). This may allow for a more systematic and consistent approach to be taken to incident reporting.

- On templates, the incident reporting template requirements set out in DORA should be consistent with notification content requirements of NISD2. The description of the content to be included in notifications is not consistent between the two proposals. It would be preferable if the notification templates for both initial and status updates do not diverge.
- DORA also enables the Joint Committee to issue regulatory technical standards with further criteria, which may cause further non-alignment at a later stage. These inconsistencies may increase the administrative burden and cost in reporting. The various supervisory authorities coordinate amongst themselves before making decisions / taking action.

Incident reporting

NISD2 changes the timeframe for reporting incidents, Article 30 obliges entities to report, without undue delay and within 24 hours, an initial notification report with information to make the competent authorities aware of the incident. This is a challenging timeframe as:

- Entities may not have ascertained within that timeframe whether an incident was "caused by an unlawful or malicious actor"
- Reporting an incident before an entity has the requisite time to patch or restore operations would actually increase the vulnerability of operators and their customers to hacker attacks
- The priority for an entity would be to rectify and restore continuity of services if disrupted

Therefore, **the American Chamber recommends that this provision is aligned with Article 33 of GDPR, where a breach should be reported without undue delay, but no later than 72 hours.**

If the European Commission seeks to introduce such summarised reporting obligations, the following steps should be taken to ensure that reporting cybersecurity incidents is efficient and effective, i.e. contributes to the overall aim of an improve EU-wide up-to-date knowledge of currently existing cyber-threat-vectors:

- the creation of an efficient, harmonised reporting channel to a competent authority (one-stop-shop principle), instead of reporting obligations to various authorities, such as competent authority for cybersecurity and the data protection officers;

- ensuring that essential and important entities can focus on measures to minimise the implications of a successful cyber incident, rather than having to fulfil reporting obligations. Therefore, companies should be required to notify competent authorities within 72 hours after identifying a successful attack, and CSIRTs should be allowed to ask for a maximum of one interim report. Moreover, since the investigation time for a complex cybersecurity incident often amount to half a year, handing in a final report after one months is not possible. Therefore, the final report should be handed in to the competent national authorities no later than one month after the entity has

finished its forensic analysis and has conducted all other measures necessary to ensure business continuity and handling the notified cybersecurity incident. Such longer deadlines for handing in a final report are pertinent to ensure that companies can focus on mitigating the cybersecurity incident in the first place and ensure the full operational capacity of a company is swiftly regained;

- an improved, daily updated, holistic situation picture as well as daily updated, sector-specific warnings, so that at least all essential and important entities can benefit from the knowledge on reported cyber-attacks and thereby, improve their own cybersecurity measures;

- a more precise definition of the term "significant incident", as the current legislative text leaves ample room for interpretation. Companies require a high degree of legal certainty, especially since essential and important entities not fulfilling their reporting obligations are liable to pay a significant fine.

Reporting potential threats or 'near misses'

NISD2 also proposes (Recital 55, and Art. 20) that entities should capture not only incidents but significant potential threats or so-called near misses in reporting obligations. **However the American Chamber stresses that increasing the threshold to near misses will likely result in an overflow of notifications and a decreased efficiency from regulators.** It also raises questions about the provenance of such information, the reliability and related liability issues. It is also impractical for entities cybersecurity teams who are consistently dealing with potential threats that 'could have potentially resulted in a significant incident'.

Entities should only have to report significant and tangible incidents, and the text outlining that entities should report 'potential' incidents should be deleted. This notification requirement should be voluntary and it is better curated in threat information sharing fora such as ISACS – this is covered in the proposal by Information sharing (Art. 26)[4].

Scope/incident notification conflict

By expanding the scope and number of service providers classified as **essential entities**, the current proposal in its current language does not take into account common practices in the enterprise cloud environment whereby one essential service provider is the user or client of another essential service provider's services. The contractual obligations of service providers in these circumstances are not

[4] Whereby, essential and important entities may exchange relevant information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. This exchange of information should take place within trusted communities and implemented through specific arrangements (entities must notify their participation in these agreements to the competent authorities). Entities outside the scope of NIS 2.0 may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses.

acknowledged, which could lead to legal ambiguity and / or overlap in reporting obligations, the cloud provider having to report an incident affecting its client to the regulator.

For example, where Company A provides essential services to its customers, using cloud computing services or infrastructure it procures from Company B - only Company A can appropriately assess the impact and gravity of an incident arising from a failure of Company B's service. Under the current proposal, Company B would be required to report to the regulator without having the necessary information or overview of the actual impact on Company A's end users. Therefore the **American Chamber recommends that there is a clarification included similar to the one in Art. 16(5) of the NIS Directive,** "[w]here an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator."[5]

In addition, liability exemptions or safe harbours for notifying incidents should be maintained in consistency with Articles 14(3) and 16(3) of the NIS Directive. Otherwise, if mandated, a reporting obligation that would go against confidentiality and contractual obligations in a typical cloud service agreement. Any deviation from this would amount to a breach of contract and the obvious risk of reputational loss for both the client and the digital service provider.

End to end Encryption (E2EE)

The proposal seems to imply that services must use encryption, including E2EE, where security principles dictate they should, however any implementation of E2EE must be balanced by the fact that law enforcement may need exceptional access; and if exceptional access is allowed, it shouldn't undermine the security benefits of E2EE. These premises are contradictory and unworkable in practice. The American Chamber recommends that the Department seek to clarify the intent of this and note that lawful intercept solutions for E2EE will inherently undermine security. Furthermore, we note that such a provision could render impossible modern SaaS features in detriment of the competitiveness and innovation of EU SMBs and recommend that this provision is deleted.

Vulnerability reporting

Vulnerability reporting rules should be amended to clarify that there is no obligation to report vulnerabilities that have not yet been patched. As outlined above with regard to the shortime for reporting incidents, reporting vulnerabilities to regulatory bodies would also increase the risk of exploitation. Indeed all information sharing of vulnerabilities is sensitive and there needs to be an

5

appropriate framework to manage the risks of increased access to such information outside of regulated entities.

Mandatory (vs. voluntary) certification

The American Chamber cautions against the introduction of mandatory certification requirements for adopted certification schemes under the Cybersecurity Act, including for cloud services, which could create market entry barriers and for small EU cloud providers that do not count on big compliance teams/resources. NISD2 should align and maintain consistency with the intention of the Cybersecurity Act wherein adopted cybersecurity certification schemes are voluntary.

If certification requirements must be made mandatory, then they should not replace existing internationally-recognized certification schemes such as ISO 27001 but only serve as an alternative.

Supervision, enforcement and fines

In line with a larger scope which classifies more service providers as essential operators, powers are also given to competent authorities to enforce a **much more intrusive oversight regime** in articles 29 and 30[6]. Likewise, Art 31.4 introduces on site audits and other measures with **potential severe penalties**, the current administrative fines outlined of up to ten million euros or 2% of total worldwide annual turnover. This is a significantly more intrusive regime than under the current Directive and other "lex-specialis" in other sectors, such as DORA for Financial Services. The punitive measures which include the option to publicly name and shame companies for non-compliance or to temporarily ban a CEO from exercising their managerial functions is not something that has been included in similar legislation such as GDPR.

The American Chamber notes that these measures and fines are disproportionate and do not offer the best incentives to achieve a productive and trustworthy collaboration between entities and authorities. Such disproportionate measures could lead to a market disincentive to use transformational technologies such as cloud computing, which has proved particularly important to allow organisations to operate in the COVID-19 environment.

Supply chain security and assessment

The attention to supply chain vulnerability is welcome, the American Chamber recommends that the Commission take into account industry led global initiatives in this area such as the Charter of Trust for Cybersecurity's recommendations for baseline security requirements in the digital supply chain. Such baseline requirements need to be supplemented by a security by design approach to products and

services. Any assessments of supply chain security should be based on substantive and not subjective grounds.

Common registry for entities maintained by ENISA

Since operators of critical infrastructures and essential services already have to register at their national regulatory authority, this proposal in Article 25 for ENISA to maintain a central registry of such entities would increase the administrative burden for the respective companies without creating any new benefit. Furthermore, the existence of a registry with information about all essential entities in the Union would in itself represent a cybersecurity risk. Therefore registration should only be at national level to avoid duplication.

Coordinated vulnerability disclosure

ENISA should refrain from publishing a biennial report that includes mainly general information. If this is to be useful, ENISA would need to publish online up-to-date information on cybersecurity incidents. A daily updated, holistic situation picture as well as daily updated, sector-specific warnings would help essential and important entities to protect their companies. If this information is gathered from other sources its utility is questionable. There are also risks of inaccurate or inconsistent reporting[7].

Management Body / Sanctions

The American Chamber recognises the step to make management bodies more responsible for the cybersecurity strategy of an essential or important entity. This step will help to significantly increase the awareness for cybersecurity issues among top-level management. However, we regard it as important that the European Commission recognises that members of management bodies of essential entities and important entities have IT security specialists that possesses the necessary qualifications to develop and implement an entity's cybersecurity strategy. Consequently, it has be questioned whether members of management bodies have to pass a respective training or whether reports by CISOs or IT security personal are not equally sufficient to provide members of management bodies with in-depth

[7] When disclosing vulnerabilities, ENISA must cooperate with the respective manufacturer of a product or the provider of a service and inform them prior to any public disclosure. Manufacturers of ICT products and providers of ICT services must have the chance to provide their customers with updates or patches to mitigate the risks of the respective vulnerability before a vulnerability is disclosed by a third party. Otherwise, hackers could exploit the disclosed information which could have serious repercussions for Europe's cyber-resilience. Therefore, a timeframe should be established for how quickly ENISA must notify the manufacturer and how long the manufacturer has to review the requests, respond to them, and roll out a bug fix if necessary.
Reporting vulnerabilities should not be a one-way road. Rather, public entities, including secret services, must be obliged to report their knowledge on vulnerabilities as well. The European Commission should include in Article 6 an obligation on government agencies from EU Members States to immediately report any information on vulnerabilities or backdoors in IT products to the respective manufacturers. Currently it is the case that government agencies frequently hold back such knowledge which represents a significant threat to Europe's cyber-resilience. This is especially the case when serious vulnerabilities in ICT products or services utilised in critical entities are concerned. Moreover, CSIRTs must never have the power to suppress or delay the disclosure of a detected vulnerability.

information. Moreover, personal accountability for non-compliance is in a step too far, especially if the goal is to ensure appropriate cybersecurity awareness in companies across sectors.

However, if the European Commission regards a mandatory IT security training necessary for members of management bodies, it should swiftly publish information on what constitutes "sufficient knowledge and skills", in order to provide guidance on which skills are considered adequate to implement the Commission's requirements. Moreover, such recommendations should be congruent across the EU in order to ensure that members of management bodies are not confronted with diverging requirements across the Single Market.

Security requirements and risk management approach

NISD2 introduces a far more comprehensive risk management approach which is generally welcomed. However, there is a risk that prescriptive requirements for security and risk management approaches will lead to security being implemented in a particular way, rather than to a particular level of assurance. Entities should be responsible for ensuring their in-scope services are delivered with an appropriate level of security, consistent with the framework under NISD2.

NISD2 introduces a far more comprehensive risk management approach which is generally welcomed. There is a risk that prescriptive requirements for security and risk management approaches will lead to security being implemented in a particular way, rather than to a particular level of assurance. Entities should be responsible for ensuring their in-scope services are delivered with an appropriate level of security, consistent with the framework under NISD2.

It may be appropriate to use the underlying international standards, schemes and protocols in this area (such as the ISO 27000 series) as examples but in doing so, **we strongly recommend that the Commission adopt an approach which recognises that how the relevant standard is met, and assured, is best determined by the entity itself and for the entity to be held accountable for those determinations.**

While industry recognises the necessity to outline basic cybersecurity risk management measures for network and information systems that all essential and important entities have to fulfil, the European Commission and Member States' governments must ensure that the IT security personnel can focus on IT security rather than on reporting obligations.

Ultimately security is implemented through a series of controls, but it should not automatically be inferred that the presence or absence of specific controls, mean that one organisation is more or less secure than another. **What is important is the outcome; that the security measures put in place by an entity are appropriate to the risks being faced**. Assurance that appropriate security is in place can be carried out in a variety of ways, one of which is to verify the presence of specific controls, but this is not the only way. For example, the use of metrics of security-effectiveness can also demonstrate that appropriate measures are in place and operating effectively.

We call on the European Commission, the European Parliament and Member States to adopt an approach which is based on appropriate outcomes, and which introduces cybersecurity risk management measures for network and information systems that provide a high degree of legal certainty for essential and important entities.

Conclusion

The American Chamber greatly appreciates the opportunity to input into this important consultation and look forward to further engagement on the topic. If the Department has any questions on the above, please do not hesitate to contact the American Chamber.