AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Towards a strong European cybersecurity environment

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3 trillion in 2020, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Introduction

The American Chamber of Commerce to the European Union supports a strong cybersecurity environment in Europe. As the EU's economy and society continues to embrace digital solutions in an accelerated fashion, the need to ensure that Europe's networks and information systems are resilient against evolving cyberattacks has never been higher. Cybersecurity is a responsibility of government and industry alike and the most effective way of advancing it is through public-private partnerships, harmonisation and global cooperation. In order to make this ecosystem thrive, it is fundamental to make security and trust a priority and to ensure the security of the entire supply chain is strengthened to avoid security risks in products and services as well as to protect customers and citizens against malpractices and abuse.

The proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive) includes a number of positive elements that could help increase cyber resilience across the EU, such as the need to address regulatory fragmentation caused by diverging national implementations of the NIS Directive (particularly regarding the identification of operators of essential services). However, **there are a number of provisions in the proposal that need improvement.** In the following paragraphs we will detail **key issues for the co-legislators to consider.** We particularly emphasise that the NIS 2 Directive should follow a risk-based approach: that is to say that requirements for companies should be targeted (no catch-all) and proportionate to the specific risks that a cyber incident impacting their services or products would entail for the economy or society. In addition, the Directive needs to be aligned with existing legislation (such as the European Electronic Communications Code [EECC][1]) as well as draft legislation (eg, proposal on digital operational resilience for the financial sector [DORA][2] and the resilience of critical entities [CER][3]).

This paper seeks to outline key recommendations regarding crucial aspects of the NIS Directive where further work remains. Our suggestions encompass the scope of the NIS Directive, focusing on how a risk-based approach should be used both in terms of identifying the essential and important entities covered but also on the proportional obligations to be placed upon them. Moreover, our recommendations point out legislative overlap and conflicting requirements to try and avoid while also offering insight on reporting obligations and thresholds. More streamlined industry involvement in efforts like the CSIRT Network and Cooperation Group could set incentives towards more voluntary information sharing. Furthermore, we offer insight on certification, international standards and encryption while advocating for caution towards the creation of a registry for essential and important entities. Crucial angles of the discussion around vulnerability disclosures, supervision and enforcement, as well as remaining issues on the provisions focusing on top level domain registration data will also be highlighted.

Scope

While AmCham EU agrees with the proposed distinction between 'important' and 'essential' entities, the same substantive requirements to both types of services is not compatible with a risk-based approach. We therefore **recommend a lighter regime for important entities** also in terms of required risk management measures and reporting. We welcome the inclusion of the public sector in the scope given their use of IT to provide public services, a large number of which are becoming critical. However, the proposal seems to use the **terms 'entity' and 'service' interchangeably**. There are cases where an entity provides one or more in-scope services while at

[1] Directive (EU) 2018/1972 establishing the European Electronic Communications Code https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN

[2] Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, and (EU) No 909/2014 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN

[3] Proposal for a Directive on the resilience of critical entities https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf

the same time providing services that are (correctly) out of the scope of the NIS 2 Directive. Therefore the **obligations of the draft Directive should not apply to the entire entity but rather to the economic unit or 'undertaking' that provides the service that is in scope of the proposed text**. This is particularly important for mixed business models between categories of activities that are described as 'essential' in the Annex and categories of activities that are described as 'important'. For instance, a technology company may manufacture robots and therefore fall into the manufacturing category of Annex 2 (important) while also developing cloud computing software to operate said robots, thus meeting the requirements of Annex 1 (critical). It is also possible that it develops on premise testing software that would be out of scope.

Manufacturing

The NIS 2 Directive is likely not an appropriate instrument to achieve the intention of the proposal regarding the inclusion of manufacturers. Ensuring the continuous and secure supply of products and services to essential entities is already addressed under the supply chain security obligation under Art. 18(2)(d). If the intention is to increase the security of products or services, it should be considered that **the purpose of the NIS Directive is to strengthen the cybersecurity of systems and not that of products and services**, which is already or will be regulated elsewhere (eg, EU Cybersecurity Act, Radio Equipment Directive, announced horizontal instrument on the security of connected devices[4]). Given the catch-all nature of the current scope, **we are doubtful as to how this could be implemented and enforced effectively in practice** without limiting and specifying this to EU-based factories/manufacturing. Moreover, the scope of manufacturing included is far too broad and will impact almost every manufacturing company in Europe and potentially outside Europe. A **much more detailed and concise description of what types of manufacturing entities should be considered important is needed**, along with **a more granular assessment of what particular manufacturing sectors should fall in the scope of the proposal.**

Cloud computing

While cloud computing is broadly in scope as an essential entity, we encourage more **specific guidance that the only cloud services deemed essential should be those whereby an outage or an incident could lead to considerable material or non-material harm**. This could be services which enable critical functions of essential entities; or where a security incident may have impact on end-users or other networks and services in scope of this Directive. The current definition of 'Cloud Service Provider' (CSP) is very broad and extends to almost all Software as a Service (SaaS) providers. Instead of adopting a catch-all approach, regulators should take into account the actual risks in case of a significant incident suffered by a CSP. In addition, the **current definition of 'cloud computing service' does not distinguish between different modes of deployment**: ie, private, community, public or hybrid cloud. In contrast to public cloud services, a private cloud offers a dedicated infrastructure to enterprise users with more control over security parameters, incident response and placement/isolation of critical applications; including scenarios where the IT infrastructure is managed or operated by the customer or a third-party service provider. Private cloud services (as stand-alone or components of hybrid-cloud infrastructures) should therefore be explicitly excluded from the scope of the Directive.

Data Centre Services

The definition of 'data centre services' should also be specified, as the sale and the actual provision of the data centre services may not be carried out by the same entity. In such a reselling scenario, the **Directive should only apply to the entity that directly provides the services to the customer**, not to the reseller of the service.

[4] JOIN(2020) 18 final, The EU's Cybersecurity Strategy for the Digital Decade

Legislative overlaps and avoiding regulatory conflicts

Policymakers should **ensure seamless and clear application between horizontal legislative proposals vs lex specialis**. The NIS 2 Directive should ensure that there are no overlaps or double reporting required amongst all horizontal and sectoral cyber related legal instruments, while at the same time acknowledging the attributes of different sectors. For example, the interaction with other regulatory instruments like DORA and the EECC (European Electronic Communications Code) needs to be clarified.

Whilst DORA foresees a clear hierarchy between DORA and the NIS 2 Directive for financial entities, it does not do the same for Critical ICT Third Party Service Providers (CTPPs). This could lead to conflicting obligations for third-party ICT providers, especially with the NIS 2 proposal. It may create a substantial overlap between the regulatory powers under the NIS 2 Directive and DORA over the same cloud and digital infrastructure providers that will be in scope of both regulatory frameworks. It is **essential for policymakers to establish a clear hierarchy between the two instruments to avoid the unnecessary duplication** and fragmentation of compliance.

With **regards to the EECC**, electronic communications service (ECS) and network (ECN) providers are already covered by strict service and network security requirements and incident reporting to competent authorities and sometimes also to their customers. Before this, ECS/ECN providers – not including interpersonal communication services – were bound by a similar set of security obligations under the previous telecoms framework. Furthermore, the NIS 2 Directive states that these rules should be repealed but leaves some uncertainty on the overlap of the legislations. It is therefore **critical to ensure the revised NIS 2 Directive provisions applying to ECS/ECN providers remain fully aligned with the text and spirit of the EECC**. In our view, **security obligations applicable to ECS/ECN operators can only be 'moved' effectively from the EECC to the NIS 2 Directive if the former's objectives, principles and safeguards are upheld too**. It is important that the EECC's key objective of harmonisation is not undermined by the NIS 2 initiative. The EECC, after all, foresees a greater level of harmonisation for the regulation of providers of ECS/ECN than the NIS 2 Directive does.

Moreover, for **cross-border over-the-top (OTT) services** (under the EECC qualified as network-independent NB-ICS or NI-ICS) which have recently been brought under the scope of the EECC, the harmonisation efforts should even go further than the EECC. We therefore strongly **recommend adding those providers under Article 24 of the NIS 2**. Any other approach risks leading to divergent, potentially overlapping and inconsistent requirements which such providers are unable to comply with (eg, different material thresholds for incident notification – as is currently the case under the EECC).

Finally, we need to **ensure complete alignment on definitions such as 'cloud computing service' and 'incidents'**, across all EU regulations (DORA, NIS 2 Directive, CER Directive, European cybersecurity certification schemes).

Reporting obligations and thresholds

Article 20 proposes 24 hours for an initial notification report to make the competent authorities aware of an incident having a significant impact on the provision of their services (hereafter referred to as 'significant incident'). Despite the minimum amount of information required, **this constitutes a very short timescale in view of the priority for businesses** to rectify the problem and restore continuity of services should such disruption occur. Exposing information about a significant incident before a patch is applied or operations restored, makes operators and their customers vulnerable to increased attacks. **Adopting the language and timeframe similar to Art. 33 of the General Data Protection Regulation (GDPR), whereas a breach should be reported without undue delay, but no later than 72 hours** would ensure harmonisation between the Union's legislative instruments and clarity for service providers. What is also unclear in Article 20 is whether the notification should go to computer security incident response teams (CSIRT) or the national competent authority (NCA). With

regards to the final report, we believe it should be provided one month after the entity has finished its forensic analysis and has conducted all other measures necessary to ensure business continuity and handled the notified cybersecurity incident as opposed to one month after the initial notification.

The **definition of a 'significant incident'** that must be reported is overly broad and vague and needs to be **clarified considering entity type and risk** based on additional parameters present in the NIS Directive (eg, number of users affected; duration; geographical spread). Moreover, Article 20 proposes to capture not only significant incidents but also significant cyber threats (that could result in a significant incident) and near misses in reporting obligations. We believe that **decreasing the threshold to significant cyber threats and near misses will likely result in an overflow of notifications** to CSIRTs and NCAs, particularly in light of the vastly increased number of entities in scope of the NIS 2 Directive. This threshold decrease would also prove a significant administrative burden for the regulators concerned. Therefore such **notification for significant cyber threats and near misses should only be voluntary**.

Disclosure of a threat or incident to the public should be the responsibility of the affected entities themselves, not the competent authorities or CSIRT. The Directive should also provide further guidance in which cases public disclosure should be considered in the public interest (eg, when it is likely to prevent actual harm or damages).

Industry involvement and information sharing

The possibility to involve industry in the CSIRT Network and Cooperation Group is a welcome proposal. This **public private relationship can be further specified in terms of a more structured engagement** (frequency, priority, etc). The first responder role of the private sector has been repeatedly demonstrated during the most critical cyberattacks including the SolarWinds attack. Secondly, CyCLONe and general cybersecurity exercises can benefit from participation of industry which could contribute with insights on threat landscape and other hands-on expertise. The early involvement and proactive development of communication channels before a crisis can significantly increase the effectiveness of the cybersecurity environment.

We also believe **more can be done to incentivise voluntary information sharing** – both voluntary reporting to government security agencies and more effective sharing of threat information by specific sectors, such as information sharing and analysis centres (ISACs). That is why we **support wider private-public information sharing and exploring the use of a sector specific ISAC model at EU level** (through what is laid out in Article 26 [3]). This exchange of information should take place within trusted communities and be implemented through specific arrangements (entities must notify their participation in these agreements to the competent authorities). Entities outside the scope of the NIS 2 Directive may submit notifications of significant incidents, cyber threats or near misses on a voluntary basis.

Notably, there are **no specific provisions to facilitate cybersecurity information processing and sharing**. Co-**legislators must provide greater clarity on how information sharing can be conducted in compliance with GDPR[5] and the e-Privacy Directive (ePD)[6]** (and in the future the e-Privacy Regulation [ePR][7] when adopted). This could include putting less risk on companies by creating specific exemptions beyond relying on the legitimate

[5] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[6] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

[7] Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

interest legal basis or advocating for approved frameworks (eg, codes of conduct) that, if used, will be prima facie evidence of companies.

Risk Management approach

The draft NIS 2 Directive introduces a more comprehensive risk management approach. 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. From an industry perspective **it is crucially important that the definitions of technical elements, formats and procedures make reference to the relevant international standards**, schemes and protocols such as ISO 27000 series which underpin global cyber security risk management practices. Reference should also be made to associated protocols and formats in common use for incident description.

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 Commission and Member States' governments must ensure that IT security personnel can focus on real-time security incidents rather than on filling in forms and being occupied by reporting obligations. We therefore **call on the co-legislators to introduce cybersecurity risk management measures for network and information systems that provide a high degree of legal certainty for essential and important entities**. Therefore, instead of referring to the 'state of the art', which leaves ample room for evaluators to conclude that not all potential state-of-the-art capabilities have been applied after an incident has happened, **reference to (minimum) standards (eg, ISO27001) should be introduced**. To this end, the Directive should **empower ENISA to adopt sector-specific guidance for Member States and companies.** Where the Commission lays down harmonised specifications in accordance with Article 18(5), it should be clarified that such specifications will replace any existing national specifications in order to avoid a duplication of requirements at EU and national level.

Certification and referencing of international standards

Since the adoption of the Cybersecurity Act (CSA)[8] in 2019, we have not seen the formal implementation of a cybersecurity certification scheme through an implementing act. Furthermore, the certification process laid down in CSA is voluntary. Cybersecurity certification schemes can play an important role in demonstrating compliance with certain security requirements - such as Cloud CSP Certifications - provided these are voluntary; developed and implemented by industry allowing for self-assessment and third-party documentation depending on the risk profile. Thus, **the obligations for essential and important entities laid down in Article 21 appear premature and too strict (mandatory/required vs voluntary)** in the current context. In addition, these are limited only to EU certification schemes which makes Europe less competitive in the international context. Mandatory certification should require retraction of national certification schemes – unless it is introduced only when national certification schemes are no longer in place. Additionally, the power of the Commission in deciding, through delegated acts, which categories of essential entities shall be required to obtain a certificate (through the existing European cybersecurity certification schemes) of Article 21 would not be proportionate. Certification schemes such as the European Cybersecurity Certification Scheme for Cloud Services [EUCS] should remain accessible to small and medium market size organisations and allow self -declaration and assessment at the basic level.

In addition, **international cyber security standards such as the ISO 27000 series, IEC 62443 or derivatives of these can be one of the main reference points for establishing compliance with security requirements for the**

[8] Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

NIS 2 Directive. Cyber attackers do not respect national boundaries. Since implementation of the original NIS Directive, new international extensions to 27000 have been added to cover cloud computing (27017 and 27018). Furthermore, ISO 27103 is a risk-based, outcomes-focused cybersecurity framework that leverages international standards relevant across sectors and could help to foster greater alignment among Member States if used for the NIS 2 Directive implementation.

Encryption

We caution against the NIS 2 Directive suggesting the need to mandate any specific security practice or technology such as end-to-end encryption. Entities should be allowed to adopt security safeguards and measures that they deem best suited for the security of their service and user's needs. Encryption should be an option for any organisation's risk management determinations. There is also the need to encourage other non-digital measures, safeguarding as well as training and better collaboration with law-enforcement. Clarity is also needed on lawful intercept requirements in end-to-end encryption and measures that would inherently undermine security of services and users must be cautioned against as they defeat the purpose of the NIS 2 Directive.

Registry for essential and important entities

Since operators of critical infrastructures and companies defined as companies of particular public interest (eg, under Germany's IT Security Law 2.0) already have to register at their NCA, (here the Federal Cyber Security Authority in Germany), this proposal for **creating a registry for essential and important entities (Article 25) would increase the administrative burden for the respective companies**. Furthermore, the **mere existence of such a registry** with information about all cyber establishments in the Union can also **in itself represent a cybersecurity risk**.

Vulnerability disclosures

We strongly support **alignment of any coordinated vulnerability disclosure (CVD) requirements with well-established and broadly adopted best practices and industry standards**, such as ISO/IEC 29147 (2018) and 30111 (2019). Any efforts around vulnerability disclosures should not be open to all 'interested' parties, as mentioned in article 6, but rather to 'selected' ones as **disclosing vulnerabilities to the wrong audience could make entities vulnerable to further targeting**.

The requirement that **ENISA establishes a European vulnerability registry in Article 6 should also be reconsidered**. Recital 31 acknowledges that other countries are doing similar work and ENISA should explore the possibility of forming structured agreements with those countries on vulnerability repositories. The global cybersecurity community has been leveraging a global Common Vulnerability Exposure (CVE) program for decades in order to track, score and streamline vulnerabilities. There are currently 157 organisations and 26 governments (and expanding) participating in this process which NIS 2 could further bolster. **International cooperation is needed to avoid confusion, duplicative work and fractured vulnerability repositories;** all of which would result in resources being unnecessarily diverted to checking multiple registries. Additionally, more specificity is needed around what scoring framework should be used to determine severity (eg, common vulnerability scoring system 3.1).

Supervision and enforcement

Enforcement provisions involving criminal liability, naming and shaming of companies/individuals or barring them from doing business or from executive office are disproportionate. This does not contribute to an equal and trustworthy relationship between the essential service providers and NCAs. We fear it leads to compliance based on less desirable incentives, such as avoiding fines or judicial processes. **Security is based on trust and cooperation should be based on equality, transparency and reciprocity**.

Furthermore, any onsite inspections or audits **should not be at random** but should be set on a periodic basis and limited in frequency to **no more than annually.** Additionally, **compulsory security scans should be removed from the proposal** as they may subject the entity to greater security vulnerabilities if the information is not appropriately protected. Article 31(4) introduces severe penalties (a maximum of at least 10 000 000 EUR or up to 2% of global turnover) for non-compliance. This is a significantly more intrusive regime than under the current NIS Directive and other *'lex-specialis'* in other sectors, such as the DORA proposal in financial services. A **proportionate sanction and oversight regime is appropriate** and would allow service providers to operate seamlessly across different sectors.

Top Level Domain (TLD) registration data (Article 23)

Since GDPR came into force in May 2018, private companies providing infrastructure for domain names have been allowed to make elective decisions about the publication and access to domain name registration data. This allows bad actors (including those conducting fraudulent commercial activities) to proliferate online with total impunity. Article 23 partly addresses this problem, requiring that entities providing Top Level Domain (TLD) registration services 'collect and maintain accurate and complete domain name registration data' and publish registration data 'which are not personal data' in order to 'identify and contact the holders of the domain names'. However, **clarity is needed regarding the notions of 'legitimate access seekers'** to whom domain name registration services would be obligated to 'reply', 'without undue delay'. Indeed, specific language concerning the justified requests of legitimate access seekers (which should include the security industry and law enforcement but also consumers and relevant industry players) is crucial to ensuring that Article 23 allows such actors to efficiently identify and take legal actions against cybercriminals. Clarification is also necessary concerning the importance of **verification of the data declared by registrants**. This could be achieved by underlining in the text the obligation for domain name service providers to verify the information of their customers (both private and professional, provided they are operating a commercial website).

However, further clarity is needed on the **scope of the DNS providers considered** under the revised Directive. **Domain name resellers and privacy/proxy registration services should be included in the final scope** (alongside domain name registries and registrars) of the Directive so as to reliably enforce requirements of accuracy; natural versus legal distinction; or prompt disclosure of personal data to third parties with legitimate interests (Article 4[9], 4[13]-[15], Article 23[1], 23[4], 23[5], Recitals 15, 61 and 62).