AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

Revision of the NIS Directive

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 U.S. positions on business matters. Aggregate U.S. investment in Europe totalled more than €3 trillion in 2019, 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

The American Chamber of Commerce to the European Union (AmCham EU) welcomes the opportunity to provide input to the European Commission's review of the functioning of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information security across the Union (NIS Directive).

As the EU's economy and society continues to embrace digital solutions, the need to ensure that Europe's networks and systems are resilient against evolving cyberattacks has never been higher. AmCham EU welcomes the role played by the NIS Directive in achieving this objective, through the introduction of concrete measures to mitigate the growing cyber threats to vital sectors of the EU economy. 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 privacy, security and trust a priority.

AmCham EU is closely following the development and further enhancement of policy tools that strengthen cybersecurity in Europe. Our members are impacted by the NIS Directive in different ways. Our membership includes Operators of Essential Services (OES), Digital Service Providers (DSPs), suppliers to both OES and DSPs, as well as companies that do not fall in these categories, or which are regulated by other sector-specific cybersecurity legislation. AmCham EU members support a strong cybersecurity environment in Europe in order to protect themselves, their customers and citizens against malpractices and abuse. Therefore, we support the European Commission's initiative to further strengthen Europe's resilience, through the revised NIS Directive and other measures.

AmCham EU's members view the 2016 NIS Directive as an effective framework which is now embedded in procedures at industry and government levels. One of the key negotiation points in the 2016 Directive was the distinction in reporting requirements between DSPs and OES. It is our view that **reporting obligations should remain as straightforward as possible**. Multiple and potentially divergent reporting requirements for an operator or a provider lead to added bureaucracy, legal ambiguity and delays. Furthermore, treating DSPs and OES in the same way undermines the criticality of OES and the need to prioritise cybersecurity on the basis of criticality. We believe it is important to keep the clear distinction between the different categories of operators and providers and their respective reporting requirements. Moreover, reporting requirements need to take into account the fact that since 2016 the legal environment of the EU has changed. The entry into force of General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) has created a horizontal reporting obligation for data incidents for all sectors. Although the scope of the NIS Directive is different, one cannot ignore that cybersecurity incidents will often involve some level of data access or misuse. Therefore, clarity on the **interplay of GDPR and the NIS Directive** on issues like security obligations, reporting obligations and cybersecurity processing, especially in the context of information sharing, would be key.

It is our opinion that **introducing targeted changes** to the NIS Directive with a view to clarifying certain provisions and improving harmonisation of the current rules **is appropriate**. We encourage the European Commission to **prioritise harmonising the process of identification of operators of essential services** to achieve better alignment across Member States, as the European Commission also concluded in its relevant October 2019 report.

We **advise against expanding the scope of the Directive to other industry sectors or services under the OES category**. We think that a strong risk-based approach and focus on operators that are essential (eg, in terms of loss of life or severe economic impact), should be retained. If more sectors are added as OES, many Member States will likely be less effective in ensuring proper implementation of the NIS Directive given the fact that the added burden to supervise and the potential information overload will exceed their capacities. We would support expansion of the scope to public administrations, due to their role as a critical infrastructure in Europe, and as long as the applicable security measures are harmonised at the EU level. However, there should be a

more exhaustive description on what type of public administration, as not all public services should be considered essential under all circumstances. The COVID-19 crisis has led to a large amount of public services (eg, schools, universities, city halls, authorities and administrations, etc) being transformed into digital services, making them potentially vulnerable to cyberattacks. The approach to identifying OES should remain proportionate to risk, and rely on criteria that are fully aligned across the different Member States to truly achieve a level playing field. In addition to maintaining the scope of OES as in the current Directive, for services operating in a cross-border manner, the nationally organised OES regime is not appropriate, and such services must be treated under a one-stop-shop regime.

The review of the NIS Directive must duly take account of existing requirements in sector specific regulations and ensure that we have alignment between the different rules and avoid overlapping, redundant or even conflicting obligations. For example, alignment should be ensured between the NIS Directive and the e-IDAS Regulation and the Directive on the identification and designation of European Critical Infrastructure (ECI Directive). This is all the more relevant as the Commission is also envisaging reviews of both the ECI Directive and the e-IDAS regulation.

In addition, market players which are already subject to cybersecurity requirements in sector-specific legislation must remain excluded from the scope of the Directive. This includes for example traditional providers of public electronic communications networks and services under the Telecoms Framework Directive, and from December 2020 such providers under the European Electronic Communications Code. This exclusion is necessary to ensure legal clarity, certainty and proportionality of obligations for such players.

Furthermore, we believe that the **current list of DSP categories, along with the security and incident notification requirements placed upon them, are appropriate**. For example, by adding other categories such as data centres, there is a risk of creating an overlap with cloud services which are already in scope (eg, Infrastructure as a Service (IaaS) is already included under cloud computing).

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). Such measures are likely to lead to a better functioning cybersecurity ecosystem between industry and governments and better preparedness for industry sectors rather than top-down legislation. While there are established mechanisms for voluntarily reporting information associated with incidents to Computer Security Incident Response Teams (CSIRTs), consideration should be given to how these existing mechanisms could be better leveraged and interplay with regulatory reporting regimes. Separating regulatory functions from CSIRTs is central to this, and this is not the case in all Member States.

The NIS Directive review provides a unique opportunity to develop a voluntary framework that will encourage direct information sharing between companies, without the involvement of national authorities. There are numerous circumstances where a company may have specific indicators of a systems compromise that would be appropriate to share with other companies. This is often information they do not want to share with a national authority. Companies should be trusted to assess when it is appropriate to share information with national authorities versus other companies.

AmCham EU encourages the European Commission to provide greater clarity on how information sharing can be conducted in compliance with the GDPR and the e-Privacy Directive (and in the future the e-Privacy Regulation when adopted). This could include putting less risk on companies by creating specific exemptions beyond relying on the legitimate interest legal basis or advocating for approved frameworks (eg, codes of conduct) that, if used, will be *prima facie* evidence of companies. **Liability exemptions,** or safe harbours, **for notifying incidents are necessary and should be maintained** in consistency with Articles 14(3) and 16(3) of the current NIS Directive.

In addition, **international cyber security standards** such as the ISO 27000 series, IEC 62443 or derivatives of these **should be the main reference points for establishing compliance with security requirements for the NIS Directive**. Cyber attackers do not respect national boundaries. Since implementation of the 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 NIS Directive implementation. Cybersecurity certification schemes can play an important role in providing security requirements, such as Cloud CSP Certifications, provided these are voluntary, developed and can be implemented by industry and allow for self-assessment and third-party documentation depending on the risk profile.

To conclude, we believe it is a **better approach to fine-tune the current Directive,** rather than to expand the obligations or rescind the Directive and move to a new Regulation. It has taken significant time for industry and governments to work together effectively to put in place all the measures required. Europe cannot afford another long cybersecurity policy debate. This is especially important in light of COVID-19, which has accelerated digital transformation throughout the EU economy and demonstrated the need to have state-of-the-art technologies to respond effectively to emerging cybersecurity challenges. There is already a strong risk that with the inevitable delay in implementation, the resulting measures could be outdated by the time they are put in place.