CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

October 2, 2020

Email: CNECT-H2@ec.europa.eu

Mr. Roberto Viola
Director General
Communications Networks, Content and Technology
European Commission
1049 Bruxelles/Brussel
Belgium

Subject: Cybersecurity – review of EU rules on the security of network and information systems

Dear Director General Viola:

The U.S. Chamber of Commerce welcomes the opportunity to provide comments on the European Commission's ("Commission" consultation of the revision of the Directive (EU) 2016/1148 concerning measures for a common, high-level of security of network and information systems across the Union ("NIS Directive" or "the Directive") aimed at fulfilling the Commission's requirements to review the functioning of the NIS Directive periodically.[1]

The U.S. Chamber of Commerce ("Chamber") is the world's largest business federation, representing the interests of more than three million enterprises of all sizes and sectors. The Chamber is a longtime advocate for stronger commercial ties between the United States and the European Union. According to a recent Chamber study jointly commissioned with AmCham EU, the U.S. and EU are together responsible for over one-third of global gross domestic product, and transatlantic trade and investment supports 16 million jobs on both sides of the Atlantic.[2] The Chamber is also a leading business voice on digital economy policy, including cybersecurity, artificial intelligence, data privacy, digital trade, and e-commerce. In the U.S. and globally, we advance sound policy frameworks that support economic growth, promote consumer protection, and foster innovation.

We appreciate the Commission's willingness to consult with industry throughout the process. The Chamber believes that considering industry voices strengthens the result. Our goal is to foster a more resilient ecosystem through the creation of industry-led, market-based cybersecurity solutions. We strongly believe that a multi-stakeholder approach to cybersecurity is the most effective way to encourage economic activity while ensuring the digital infrastructure's security.

[1] European Commission. *Directive (EU) 2016/1148*. https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[2] U.S. Chamber of Commerce and AmChamEU, *The Transatlantic Economy 2020*. https://www.uschamber.com/sites/default/files/te2020_report_final.pdf

The Chamber recognizes that managing cyber risk in all network and information system sectors is vital to the U.S. and Europe's economic and national security. The European Union's (EU) first cybersecurity legislation has improved Member State capabilities, increased EU-level cooperation, and established a common, high-level of security for covered entities. The Chamber applauds the work of the computer security incident response team (CSIRT) network and the NIS Cooperation Group, which have enhanced Member State and EU-level cybersecurity capacity. Further, enhancing the overall level of cybersecurity across the internal market was the passage and implementation of Regulation (EU) 2019/881 (the "Cybersecurity Act") supports the EU Agency for Cybersecurity (ENISA) and the establishes a public-private framework for the certification of products, services, and processes.[3]

The Chamber appreciates the importance and positive outcomes associated with the implementation of the NIS Directive. However, we would like to re-emphasize several fundamental principles as the Commission evaluates the NIS Directive's functioning. In a constant and significantly evolving technological and threat landscape, the Chamber believes that the following recommendations will further build on the effectiveness, efficiency, coherence, and relevance of the NIS Directive.

Enhancing International Collaboration and Alignment.

The Commission's goals with the NIS Directive, and the Cybersecurity Act that followed, established common, high-level security across the digital single market for operators of essential services (OES) and digital service providers (DSP) and future ICT products, services, and processes for cybersecurity certification. The Chamber believes that future EU cybersecurity policies, procedures, and regulations should promote international alignment and interoperability with industry-backed approaches to risk management to the maximum extent possible.

The Chamber recommends that security measures be based on industry-led international technical standards and frameworks. The Chamber strongly urges the Commission to build on and not duplicate existing frameworks and best practices. OES and DSP entities benefit when governments leverage existing cybersecurity frameworks and international technical standards as a starting point.

Examples include:

- U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework.[4]
- International Organization for Standardization/ International Electrotechnical Commission ("ISO/IEC") 27001:2013, ISO/IEC 27103:2018, or ISO/IEC 27101 (a forthcoming standard that incorporates ISO/IEC 27103:2018).

[3] European Commission. *Regulation (EU) 2019/881*. https://eur-lex.europa.eu/eli/reg/2019/881/oj
[4] U.S. National Institute for Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity (2014). https://www.nist.gov/cyberframework

Given that organizations across critical sectors use the NIST Cybersecurity Framework, ISO/IEC 27103, and ISO/IEC 27101, the Chamber urges the Commission and ENISA to continue to promote their use as they are essential for interoperability across regions and interdependent sectors. For technology providers, ISO/IEC 27001:2013 also provides foundational guidance and assurance artifacts that can strengthen security and efficiency. These common, high-level security standards allow an organization to scale its compliance programs regardless of jurisdiction.

The Chamber recognizes ENISA's guidelines to OES and DSP on assessing their compliance with NISD security requirements and incident reporting.[5][6][7] The mapping of security measures for OES and DSP to international standards used by covered entities is both useful and welcome. However, we reiterate the importance of harmonization across the EU and the importance of common, consistent, and interoperable security measures. We urge the Commission to minimize the regulatory overlap and confusion, including among existing and future frameworks.

Emphasize capacity building and information sharing.

Public and private entities are vulnerable to attempts by a malicious cyber actor to attack the confidentiality, integrity, and availability of networked systems. Cyber risk cannot be entirely eliminated but must be managed or transferred. As part of sound enterprise risk management and defense in depth processes, information exchange (i.e., cyber threat information sharing) can improve and safeguard networks and information systems.[8] The Chamber encourages further capacity-building and information sharing between private to private entities (e.g., OES to an information sharing and analysis center or sector colleague) and between private entities and government bodies (e.g., OES to computer security incident response team).

We believe that incentivized voluntary information sharing makes companies and governments alike stronger while weakening adversaries and bad cyber actors. We encourage active sharing of threat intelligence and known vulnerabilities between relevant stakeholders as a critical aspect of protecting OES and DSP entities and strengthening the ecosystem's defense against bad actors. The Chamber views incentivized voluntary information sharing as a more productive means of reporting to government security agencies and more effective sharing of threat information by sector-specific information sharing and analysis centers (ISACs). Each approach is essential and will lead to more operational cybersecurity ecosystem between industry and government and better preparedness for industry sectors.

---

[5] ENISA. *Guidelines on assessing DSP security and OES compliance with the NISD security requirements* (2018). https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements

[6] ENISA. *Mapping of OES Security Requirements to Specific Sectors* (2018). https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors/

[7] ENISA. *Minimum Security Measures for Operators of Essentials Services* (2019). https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

[8] The Chamber defines cyber threat information as structured information like signatures, indicators of compromise and unstructured information like defensive measure, vulnerability information, remediation

Possible EU-level incentives include industry protections from liability, regulatory, disclosure, or antitrust issues when sharing cyber threat information with industry peers, CSIRTs, or competent authorities. Improving the sharing of real-time data—including classified information—will foster trust and operational collaboration between network defenders and governments. In this regard, establishing policies, plans, and procedures for collecting, detecting, identifying, disseminating, and rapidly declassifying information on cyber threats should be an EU-level and Member State priority. Companies at risk naturally gravitate towards public and private entities with real-time information that enables them to stay one step ahead of malicious actors.

Requirements for Security and Incident Notification.

Article 14(3) stipulates that an OES notify, without undue delay, the competent authority and the CSIRT in case of an incident that significantly impacts the continuity of an essential service. A similar mandatory reporting structure applies to a DSP under Article 16(3). While the Chamber respectfully opposes global and domestic government mandates for cyber incident reporting, we recognize that in a certain number of limited instances they are required. In these targeted circumstances, thresholds for mandatory reporting should capture only high-risk, high-speed, and high-impact cyber incidents that may have cascading international impact. These kinds of incidents are rare, but due to the potential geographic spread and potential for the interruption in essential services a genuine public-private response is required. The Chamber believes that this kind of operational collaboration is achieved over years of joint risk management activities, and not through a forced reporting structure. Overly broad incident reporting requirements that capture network pings or other common deflections at the network edge, for the purposes of building trend reports, violate sound cyber risk management principles and unravel the consensus that information sharing between industry and the government must be based on collaborative partnerships to work effectively.

The Chamber thanks the Commission for the opportunity to provide these high-level views. We expand on these views in greater detail in our answers to a select number of the Commission's survey questions (attached). The U.S. business community is engaged in significant trade and investment with the European Union and is proud of its continued contributions to our vibrant bilateral commercial relationship. We look forward to continued dialogue on the Commission's NIS Directive consultation, as well as other foundational digital policy issues.

If you have any questions or if we can clarify our positions, please contact Vince Voci (vvoci@uschamber.com) and Abel Torres (atorres@uschamber.com).

Sincerely,

Abel Torres
Senior Director
Center for Global Regulatory Cooperation
U.S. Chamber of Commerce

Vincent Voci
Executive Director
Cyber, Intelligence, and Supply Chain Division
U.S. Chamber of Commerce

Enclosure:

1. U.S. Chamber of Commerce Consultation on the revision of the NIS Directive Survey Responses

Cc: Khalil Rouhana, Jakub Boratynski

Enclosure:

U.S. Chamber of Commerce Consultation on the revision of the NIS Directive Survey Responses

Sub-section 1.c. – Technological advances and new trends

Q1: In which way should such recent technological advances and trends be considered in the development of EU cybersecurity policy?

[Answer]: The Chamber believes in a regulatory framework that fosters secure and trusted technologies that power the digital economy. Future frameworks should build on sound secure-by-design principles and endorse flexible cyber risk management approaches that can evolve to address new and emerging threats. We support technology-neutral, risk-based approaches, and driving cybersecurity priorities and investments with outcome-driven policies.

Sub-section 1.e. – Sectoral Scope

Q3: Do you consider that also other sectors, subsectors and/or types of digital services need to be included in the scope of the Directive due to their exposure to cyber threats and their importance for the economy and society as a whole?

[Answer]: The Chamber believes that the directive's sectoral scope is adequate as it stands and should not be expanded to other sectors or services under the OES and DSP categories. Expansion of either of the categories will not improve cybersecurity resilience. The current compliance requirements have taken years to imbed in company procedures. Expansions in scope will lead to additional bureaucracy and overhead and divert existing resources away from critical functions. Furthermore, the Chamber believes that there is sufficient flexibility in the NIS Directive for the Member States to denote what infrastructures are essential to their national and economic security. The Commission's expansion considerations for additional categories should solely be based on risk and based on evidence rather than political design.

Sub-section 2.i. – Information exchange

Q2: Should the Cooperation Group be assigned additional tasks so far not listed in the NIS Directive?

[Answer]: Yes, the Cooperation Group has been a useful instrument in building capacity and sharing best practices across the Members States. We recognize that the NIS Directive supports public-private cooperation. We suggest that operational collaboration expands between covered entities and the Cooperation Group regarding equality, transparency, and interoperability. The Chamber offers two examples for the Commission's consideration.

First, either the NIS Directive Cooperation Group, the CSIRT Network, or ENISA could host an annual public-private meeting to discuss cybersecurity, share best practices, and identify possible cooperation. Both the CSIRT Network and NIS Cooperation could be required to organize such an event and make it part of their annual work programs. Doing so would benefit and increase the cybersecurity competence of the EU.

Secondly, the Commission could establish a NIS Industry Stakeholder Group, either separately as a third pillar next to the CSIRTs Network and Cooperation Group, or even as an advisory group to the NIS Cooperation Group. Such an Industry Stakeholder Group should be capable of assisting ENISA, the Member States, and the Commission to draft technical documents and providing evidence and experience in critical information infrastructure protection based on OES and DSP experience. This group should consist of both OES and DSP representatives that fall under the NIS Directive scope. The Chamber looks at the Stakeholder Cybersecurity Certification Group under Article 22 of the Cybersecurity Act as a model body for public-private collaboration.

Sub-section 2.k. – Coherence of the NIS Directive with other EU legal instruments

Q1: To what extent are the provisions of the NIS Directive (such as on security requirements and incident notification) coherent with the provisions of other EU legal instruments that are aimed at increasing the level of data protection or the level of resilience?

[Answer]: The Chamber urges the Commission to harmonize any changes to the NIS Directive with future legislation, such as Digital Operational Resilience Act, to avoid duplicity and confusion in the market place. DORA, among other requirements specific to the financial sector, establishes both incident reporting and information sharing mechanisms.

Sub-section 3.a. – Provision of cybersecurity information

Q1: How could organizations be incentivized to share more information with cybersecurity authorities on a voluntary basis

[Answer]: In the U.S., the Cybersecurity and Information Sharing Act of 2015 establishes a voluntary, protected, and bidirectional cyber threat indicators and defensive measures sharing program that protects privacy and civil liberties.[9] Participation in the Automated Indicator Sharing program incentivizes federal, but not law enforcement or Department of Defense agencies, and non-federal entities to exchange information, in real time, by protecting entities from disclosure, regulatory, or antitrust issues. Realtime sharing of common, easy to identify cyber threats enhancing situational awareness across the ecosystem, while allowing network defenders to focus on harder to defend advanced and persistent threat actors. The Chamber urges the Commission to codify in legislation a similar voluntary, protected, and incentivized information exchange program.

While governments (*e.g.*, computer emergency response teams, national cybersecurity centers) and industry (*e.g.*, commercial off the shelve threat intelligence providers, information sharing and analysis centers) routinely sharing cyber threat information with private sector stakeholders, this information is structured and formatted. In contrast, threat data on vendor- or product-based risk (e.g., the insertion of malicious code or other forms of compromise or exploitation) is not widely available.

[9] Cybersecurity and Information Sharing Act of 2015. Public Law 114-113. https://www.govinfo.gov/content/pkg/PLAW-114publ113/html/PLAW-114publ113.htm

Future information exchange programs with critical technologies supply chains may consider the following:

(1) What supply chain information would be most valuable for the Government and industry to mitigate the risk of sabotage?

(2) Does such information exist in a public or private body or sharing platform that allows it to be accessible across the supply chain for risk management purposes?

(3) How will competent national authorities share targeted intelligence and involve relevant suppliers in assessing risks to specific products?

(4) What legal or policy barriers to bi-directional information sharing exist, including substantial countervailing risks of IP loss and inadvertent dissemination of security vulnerabilities?

The Chamber firmly supports the notion that a real-time threat picture, including intelligence insights and tactics, techniques, and procedures, will empower OES and DSP to take appropriate and timely risk management actions.

Q2: Under the NIS Directive, Member States shall require companies to report events having an actual adverse effect on the security of network and information systems (incidents). Should the reporting obligations be broadened to include other types of information in order to improve the situational awareness of competent authorities?

[Answer]: No, forced reporting requirements should be appropriately limited, narrow, and targeted to cyber incidents that have evidence of serious or significant harm to the national and economic security of Member States. These arrangements are flawed for several reasons, including:

- First, mandatory reporting insufficiently considers the increased costs and misallocated businesses' resources (*e.g.*, human and technical) due to forced reporting.

- Second, the Chamber rejects policies that require reporting on a fixed timeframe. Among other considerations, what may be understood in the first few days of a cyber incident investigation can be dramatically different from what is learned in the weeks and months that follow.

- Third, several critical infrastructure sectors (e.g., financial services and energy) have existing legal obligations to report significant cyber incidents to government regulatory bodies. It is challenging to discern what increased value would flow to the national competent authorities, CSIRTS, and other sector specific government agencies when such information is seemingly available.

- Fourth, we believe that liability exemptions or safe harbors for reporting incidents are necessary and should be consistent with Articles 14(3) and 16(3) of the NIS Directive.

Sub-section 3.c. – Vulnerability discovery and coordinated vulnerability disclosure

Q3: How would you describe your experience with vulnerability disclosure in the EU and how would you improve it?

[Answer]: The NIS Directive should continue to focus on security measures for covered entities and the reporting of significant cyber incidents that could substantially impact the Member States. Over time, there may be updates to baseline security requirements that reflect the changing threat landscape or technology ecosystem; however, potential additions should be carefully evaluated to understand their likely impact. When addressing vulnerability disclosure, we urge EU institutions to utilize well-established and broadly adopted best practices and industry standards in the field of coordinated vulnerability disclosure (CVD) and vulnerability handling. The Chamber supports full alignment with these practices, as articulated in international standards such as ISO/IEC 29147:2018 and ISO/IEC 30111:2019, given the global nature of technology development and vulnerability management processes.

Q4: Should national authorities such as CSIRTS take proactive measures to discover vulnerabilities in ICT products and services provided by private companies?

[Answer]: Encouraging the adoption of CVD policies would foster better security practices among covered entities and give covered entities time to build complex and resource-intensive programs. However, prematurely requiring such policies across sectors, including those in which organizations have had limited interaction with security researchers and vulnerability reporters and limited experience receiving external vulnerability reports, may undermine the communication and cooperation essential to a positive security outcome. Any implementation of proactive measure should therefore reflect the maturity level of all stakeholders involved.

Sub-section 3.d. – Security of connected products

Q1: Do you believe that there is a need of having common EU cybersecurity rules for connected products placed on the internal market?

[Answer]: Defining minimum and common cybersecurity baselines could help improve resilience in the current digital environment, and in that regard, the Chamber support EU-level coordination. However, the NIS Directive does not seem the right instrument to address this issue. The NIS Directive was not scoped to cover ICT products, services, or processes, like consumer connected products. Developing security-by-design processes and self-assessment frameworks (e.g., GSMA IoT Security self-assessment framework), based on globally-adopted and industry-driven practices and standards, could help to promote cybersecurity capabilities and increasing participation of companies of all sizes. The Chamber supports international efforts aimed at aligning regulatory approaches to reflect accepted best practices. Private industry benefits when governments incorporate existing cybersecurity frameworks. Further, we recommend that both definitions (e.g., for devices, passwords, updates, etc.) and security requirements align with international standards such as ISO/IEC 27402 (under development) to avoid technical barriers, as well as unintended costs. However, where standards are minimum baselines, manufacturers should be encouraged to strive for greater security.

Additionally, NIST is developing "Recommendations for IoT Device Manufacturers," and recent drafts align with the risk-based measured approach for which the Chamber advocates. Other sources of existing cybersecurity frameworks and best practices include: NIST Framework for Improving Critical Infrastructure Cybersecurity; Council to Securing the Digital Economy C2 Consensus on IoT security core capabilities baseline; and NISTIR 8259.