CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

1615 H Street, NW
Washington, DC 20062-2000

September 30, 2017

Via niscallforviews@culture.gov.uk

Stuart Peters
NIS Directive Consultation (4/49)
Department for Digital, Culture, Media, & Sport
100 Parliament Street
London
SW1A 2BQ

Subject: Consultation on the Security of Network and Information Systems Directive

Dear Mr. Peters:

The U.S. Chamber of Commerce is the world's largest business federation, representing the interests of more than 3 million businesses of all sizes, sectors, and regions, many of whom are major employers and provide significant investment in the U.K. economy. We welcome the opportunity to provide the following comments as part of the public consultation on the Security of Network and Information Systems Directive (NIS directive).

The Chamber congratulates the Department for Digital, Culture, Media, & Sport (DCMS) for their leadership and private-sector engagement throughout the transposition of the NIS directive process. While there are many aspects of the public consultation that are positive, we believe that certain changes are needed. We offer the following comments and recommendations:

- **Ensure that the definition and designation of operators of essential services (OES) and digital service providers (DSP) are clear, appropriately limited, and consistent.** We agree with the core objective of the NIS directive, which is to enhance the security of network and information systems for OESs and DSPs. The Chamber urges the U.K. government to strictly limit identification to a small number of entities. We urge national competent authorities (NCAs) to apply a rigorous, proportionate, and risk-based analysis to determine what should be designated an OES or DSP.

- **The level of penalties is overly punitive and counterproductive.** The major fines envisioned included in the public consultation are likely to create an environment of mistrust between OESs and DSPs which could negatively impact voluntary cyber threat information sharing if organizations fear regulatory impacts or penalties. In addition, the scale of potential fines may serve as a disincentive to future and current investment in the U.K. This is particularly the case in a European context, as other major European economies have opted to cap penalties at far lower rates (e.g., Germany has capped penalties at €50,000). The U.K. government should bring NIS directive penalties to a

lower, more reasonable level, in conjunction with those of the General Data Protection Regulation (GDPR).

- **Security measures must leverage existing best practices and global industry-led standards.** Any cybersecurity framework is most effective when developed in collaboration with the private sector, adopted on a voluntary basis, and recognized globally. The U.K. should align any practices and standards it issues with industry-backed approaches to risk management, such as the ISO/IEC 27000 family of information security management systems standards or the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*. Allowing OES to combat evolving cyber threats with evolving best practices and standards permits a more flexible, current, and risk-based approach to cybersecurity.

- **Mandatory and broad incident reporting requirements can be counterproductive.** Frameworks that force companies to report cybersecurity incidents without clearly defined risk-based criteria, leaving broad thresholds for reporting, can unintentionally inhibit cybersecurity by causing companies to notify regulators of *any* incident on their systems. This can lead to notification fatigue, increased costs, and operational distractions, which makes it difficult to identify and address the most important incidents. Notification requirements should avoid narrow timelines and instead focus on facilitating the ease and speed with which notifications can be made.

- **Cybersecurity incident reporting is distinct from cybersecurity threat sharing**. The former occurs after an incident has happened, whereas the latter is proactive, informing organizations of potential threats (e.g., malicious code, indicators of compromise and tactics of cyber criminals) so that organizations can protect and defend their networks. As the U.K. government transposes the NIS directive into national law, we urge you to add a mechanism for cyber threat information sharing that includes the following parameters: multidirectional cyber threat sharing (e.g., government to industry, industry to industry); voluntary sharing of information; and protections from liability (including liability under data protection and anti-trust laws) when sharing information with industry peers or governments.

- **Transparency and public-private partnership are essential.** As the U.K. moves forward with transposing the NIS directive into legislation, any changes to codes of practice, standards, incident reporting, and essential services should include a public consultation before amendments are made.

- **Transition period.** The Chamber urges DCMS to apply a transition period for OESs and DSPs similar to those provided under U.S. legislation and NCA security measures guidance. This would give covered entities additional time to comply with these new requirements.

The attached questionnaire response explains our concerns in greater detail, seeks clarification on several provisions, and offers our recommendations.

Sincerely,

Ann M. Beauchesne
Senior Vice President
National Security and Emergency Preparedness
U.S. Chamber of Commerce

Sean Heather
Vice President
Center for Global Regulatory Cooperation
U.S. Chamber of Commerce

U.K. NIS Directive Implementation Strategy Public Consultation

Essential Services

1. *Are the identification thresholds set at a level that captures the most important operators in your sector based on their potential to cause a significant disruptive effect if disrupted? YES/NO*

   No/unclear.

2. *If not, why not? What would you change and why? Narrative response?*

   While the proposed thresholds capture major operators in each sector, greater clarity is needed regarding how this will be applied to the essential services supply chain.

National Framework

3. *Do you agree with the government's proposed approach of adopting a multiple competent authority model. YES/NO*

   Yes.

4. *If not, why do you believe a single competent authority model represents a better option? Do you have an alternative outside of these two models? Narrative answer.*

   The U.S. Chamber supports a multiple competent authority model which enables the U.K. government to take a more nuanced, sectoral approach to cybersecurity. Given that many companies will operate across multiple sectors, however, we would encourage the development of mechanisms for liaison between competent authorities that have shared-jurisdiction over a single company. This will ensure that requirements made of said company do not conflict and enable compliance with all relevant competent authorities.

   In addition, we welcome the establishment of a centralized mechanism for incident reporting to ensure that companies are not overburdened by compliance procedures in the midst of an intrusion. We understand that various technical solutions currently being explored by the U.K. government and would encourage you to consult with stakeholders on a technical level during the development of such a mechanism.

5. *Is the proposed competent authority for your sector a suitable choice? YES/NO*

   YES

   In the current proposal, the ICO is the UK National Competent Authority (NCA) for DSPs. While this could be appropriate, the resourcing and operational mandate of the NCA will impact whether it is a suitable choice. Any NCA must have the necessary technical expertise, physical infrastructure, and other resources for network and information security. In addition,

there must be clear boundaries between its operation of any mandatory incident notification regime and existing, voluntary information sharing between industry and government, which is often based on trusted relationships that are established over time.

As such, the Chamber encourages the UK Government to ensure: (1) the ICO is given appropriate infrastructure and resources; and (2) there is clarity regarding the roles and responsibilities of various stakeholders, such as the national CERT, the NCSC, and the ICO, and existing voluntary, trust-based information sharing and mandatory incident notification. Clear separation between these processes is necessary to avoid potentially detrimental effects on the preservation of existing trust networks.

Security Requirements for OESs

7. *Do you believe these high level principles cover the right aspects of network and information systems security to ensure that risks will be appropriately managed? YES/NO*

   Yes.

8. *If NO, can you clarify what aspects you believe are missing and recommend how we could address these? Narrative answer*

   In order for organisations to fully understand whether they are compliant, further clarification as to what outcomes they must meet is required. Most international organisations align to international standards, such as ISO 27001, or risk management frameworks like the U.S. National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*. As such, the ability to leverage existing, industry-supported standards and risk management frameworks is important if best practices are to be scaled into the U.K. market.

   Furthermore, it would be helpful if the U.K. government could clarify whether and how OES security requirements will flow through the supply chain. Specifically, are OESs responsible for ensuring that companies with whom they interact are compliant or will this responsibility fall to those companies?

9. *Do you believe these principles would impose any additional costs on designated operators, or on the sectors in scope as a whole? YES/NO*

   Yes.

10. *If YES, what do you consider would be the anticipated resource implication on designated operators, or on the industry as a whole of meeting these principles? Are you able to elaborate on the nature of these costs? Where possible please detail any specific financial costs you consider would likely result. Narrative answer*

    There will inevitably be an increase in cost to meet new security requirements, the scale of which depends on the detailed requirements of companies, which are yet to be published. At

the very least, additional staff will be required to service the new regulation and support interaction with the competent authority or authorities.

One way to limit these costs would be to develop mutual recognition-style systems with other European governments who have implemented the NIS Directive and where a company has utilized the same approach to cybersecurity in both markets. We encourage the U.K. government to explore this and other opportunities to control the compliance costs imposed on OESs.

11. *Do you have any plans to make additional security related investments as a result of this Directive? Where possible please indicate the size of investment (in £)? YES/NO*

    Yes (probably)

12. *If YES, please provide the amount and details of what investments would be required. Narrative answer*

    While many companies have comprehensive security investment programs, it is difficult to understand if they will face security gaps, requiring additional investments, without more specific details of the required controls arising from the legislation.

Incident Reporting for OESs

13. *Do you consider these incident reporting proposals to be reasonable to ensure that serious incidents affecting the network and information systems of essential services are reported? YES/NO*

    No.

14. *If NO, why not? Can you suggest revised incident reporting proposals that ensure serious incidents are reported? Narrative answer*

    The provisions for ongoing threat information sharing are a positive development and will provide an important contribution to increasing cyber resilience. Nevertheless, it is important that such programs remain voluntary in order to avoid, on the one hand, creating too much 'noise' – by preventing stakeholders from using discretion in terms of what they share – and, on the other hand, diverting resources away from cyber risk management by placing onerous requirements on businesses to report every attempted intrusion.

    The statement that "the voluntary reporting of such incidents will not subject OES to increased liability" is welcome, though we would urge greater clarification as to what legal protections will be provided for private sector entities. In particular, while information submitted to the NCSC will be protected from Freedom of Information requests as it falls within GCHQ, will this protection extend to the subsequent dialogue with regulators around such incidents? We would welcome efforts to ensure that this is the case, given that OES-regulator trust is so critical to facilitating a strong dialogue on the issue of cybersecurity.

With regards to the definitions of "an incident" and a "significant impact" – the conditions on which the triggering of incident notifications will be predicated – we believe that the current definitions are still somewhat ambiguous. Understanding that greater clarification will be provided in the coming months, we would encourage the U.K. government to ensure that OES stakeholders are consulted, along with the NCSC and competent authorities, in the development of subsequent guidance.

Finally, the establishment of a single point of contact for incident reporting – the NCSC – is a positive development which should both decrease the burden on OESs operating in a number of sectors, and ensure that the NCSC has visibility into all threats which are impacting these sectors.

Due to the sensitive nature of the breaches to be notified to the competent authorities, organizations would require assurance that security notifications and control information will be kept confidential and will not be subject to the Freedom of Information Act. This is currently the case when such incidents are reported to the NCSC.

15. *Do you consider that the proposed timeframe for providing incident reports place an undue burden on designated operators of essential services? YES/NO*

    Yes.

16. *If YES, can you explain what these burdens and costs would be? Narrative answer*

    The 72-hour maximum reporting period places an unrealistic burden on Operators of Essential Services. Given the limited time period, they will likely not be able to provide a complete picture of what has occurred, diminishing the utility of incident reporting. We recommend that the language be adjusted to align with Article 33 of the GDPR and state that reporting should be conducted "without undue delay and, *where feasible*, not later than 72 hours after having become aware of it." In addition, we would urge the U.K. Government to adopt the GDPR's provision for organisations to report outside of this timescale where they provide adequate reasons for any delay.

    While all efforts should be made to provide timely notification of cyber breaches, reporting timelines should be such that companies have time to gather critical information. In the wake of a cyberattack, companies need to determine its nature, source and impact on their systems, while coordinating rapid and sufficient response. This situation places extreme pressure on cybersecurity officers, which is further exacerbated by narrow windows for notification. Notification requirements should therefore avoid narrow timelines and instead focus on facilitating the ease and speed with which notifications can be made.

Digital Service Providers

17. *Are Digital Service Providers easily able to identify themselves using these criteria? YES/NO*

No

18. *If NO, Why Not? Can you provide revised criteria that would identify providers more easily? Narrative answer*

The definition of a cloud computing service should more clearly distinguish between the various levels of criticality associated with different types of cloud services. International standards, and in particular ISO 17788:2014, provide clarity based on cloud capability type (i.e., application, platform, or infrastructure) and thus reflect criticality considerations. Infrastructure as a Service (IaaS) acts as a foundation for Platform as a Service (PaaS) and Software as a Service (SaaS) offerings as well as other digital services; as such, its criticality may be greater than PaaS or SaaS. Moreover, there is great diversity in SaaS offerings, and considering them equally critical to the infrastructure on which they run may distract attention from more significant incidents.

Penalty Regime

29. *Do you consider the proposed penalty regime to be proportionate to the risk of disruptions to operators of essential services? YES/NO*

No.

30. *Do you believe that the proposed penalty regime will achieve the outcome of ensuring operators take action to ensure they have the resources, skills, systems and processes in place to ensure the security of their network and information systems? YES/NO*

No.

31. *If you answered NO to either of these two questions, please explain how the penalty regime could be amended to address your concerns. Narrative answer*

While financial incentive structures can be powerful motivators, policymakers should note that significant market-based incentives already exist. Moreover, as cyber awareness increases among consumers, shareholders and hackers, so too will the incentives. If regulators wish to motivate companies, they would be better served to promote cyber awareness than to impose overly burdensome penalties on the already overburdened victims of cyberattacks.

The level of penalties outlined in the public consultation is not only overly punitive towards the victims of cyberattacks, it may have a multitude of impacts which are counter-productive to the broader intent of the legislation.

Firstly, the potential imposition of major fines could undermine relations between OESs and DSPs on the one hand, and regulators on the other, as well as a creating a chilling effect on reporting. Their existence is likely to create an environment of mistrust on the part of private sector entities, which could undermine the kind of information sharing outlined in our

response to Question 14, thus undermining broader efforts aimed at increasing cyber resilience.

Secondly, the imposition of major fines in the wake of a major cyberattack could place an OES at risk financially. This prospect creates an incentive for hackers to specifically target those entities in order to destabilize the broader economy. While no public list of OESs will be made available, in most cases malicious actors will be able to deduce their status according to the publicly available thresholds and act accordingly.

Finally, the scale of potential fines may serve as a disincentive to future and current investment in the U.K. This is particularly the case in a European context, as other major European economies have opted to cap penalties at far lower rates – in Germany's case, at €50,000 and €100,000.

While the U.K. government's rationale – that a significant cyberattack is of at least as great importance as a data protection breach and therefore penalties should match those of GDPR – seems plausible on the surface, we would caution that two wrongs do not make a right. In this case, should the U.K. government insist on parity between the two, it is within its power to lower the penalties for both GDPR and the Security of Network and Information Systems legislation to a more reasonable level.