Brussels, 30 September 2017

BSA | The Software Alliance's feedback on the UK Government Consultation on the Security of Network and Information Systems Directive

BSA | The Software Alliance ("BSA")[1], the leading advocate for the global software industry, welcomes the opportunity to provide its views on the Department for Digital, Culture, Media & Sport's ("DCMS") public consultation on the 'Security of Network and Information Systems Directive'. BSA supports the efforts of the United Kingdom ("UK") to ensure that the UK is secure and resilient to cyber threats and welcomes the intention that on exit from the European Union ("EU") the Network and Information Security ("NIS") Directive will continue to apply in the UK.

BSA supports the assessment by the UK Government that the 2016 UK Cyber Security Strategy ("UK Strategy") largely addresses the requirements of the NIS Directive. Those requirements which are not sufficiently covered by the UK Strategy should be properly addressed through a NIS specific addendum. BSA encourages DCMS to develop any NIS specific addendum in consultation with stakeholders to ensure that all interested parties are able to express their views.

As the UK Government continues to consider the implementation of the Directive, we wish to provide the following comments:

1. **Competent Authority Model** – The UK Government should pursue a single competent authority model based around an authority capable of effectively assisting and improving the network and information security of organisations. The NCSC is best fit to assume this role.

2. **Security Requirements for Digital Service Providers** – The UK Government should clarify that none of the suggested security elements are binding in nature and that Digital Service Providers ("DSPs") retain flexibility in how they implement their baseline security measures. In addition to measures drawn on ISO 27001, the UK Government should also recognise the equivalence of the baselines set out in the "Framework for Improving Critical Infrastructure Cybersecurity" issued by the U.S. National Institute for Standards and Technology ("NIST") and the UK Government's "Cyber Essentials" framework for purposes of NIS compliance.

[1] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the internationals marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.*
BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Intel, Intuit, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Tend Micro, Trimble Solutions Corporation, and Workday.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

3. **Incident Reporting for DSPs** – The UK Government should ensure that incident reporting focuses on the principle of availability and avoids referencing integrity and confidentiality. The introduction of arbitrary quantitative thresholds should also be avoided.

4. **Penalties Regime** – The UK Government should revisit the proposed penalties regime and seek to align the framework with "administrative fines", in line with other consumer protection penalties regimes. Business should also be reassured that they will not be fined under both the GDPR and Directive for the same incident.

Issues and BSA Positions

1. Competent Authority Model

BSA recognises the merits put forth by the UK Government in its proposal to pursue a multiple competent authority approach. While such an approach may ensure that each nominated authority has experience working with their respective sectors, BSA believes that a **single competent authority model would effectively ensure consistency across the economy when dealing with incidents, enforcement and penalties.**

Establishing a single competent authority would allow for a consolidated centre of information with expertise across industry sectors. Such cross-industry expertise is important because attacks often shift across sectors, developing upon the success of earlier intrusions. When faced with such an attack, a model where each sector reports incidents to different competent authorities will likely prove ineffective as information sharing will likely not occur in a timely enough manner. As many multi-sector attacks often follow a given pattern, it will be difficult to decipher its development if all information is not centralised with one authority.

Furthermore, we question whether separate sectoral authorities would all be able to reach the appropriate level of skills and expertise needed to handle incidents and effectively share critical information to ensure detection and deterrence across the economy.

Moreover, a **multiple competent authority approach would lead to unnecessary complexity for those DSPs whose services span multiple sectors**. The potential designation of numerous competent authorities, together with the maintenance of an existing relationship with the National Cyber Security Centre ("NCSC"), would prove overly burdensome and not in line with the objectives of the Directive. BSA would welcome further clarity on how a DSP would be able to identify its competent authority in such a circumstance.

While BSA understands the reasoning for the potential selection of the Information Commissioner's Office ("ICO") as the competent authority for DSPs, we believe the **NCSC would be the most suitable body to carry out this role**. The implementation of the Directive should seek to designate the competent authority with the highest level of expertise in the field of cyber. While the ICO is well respected within the field of data protection, it has little experience in aiding

organisations in detecting, deterring and defending against cyber-attacks. Instead the UK Government should focus on further developing the NCSC to act a model for other EU Member States to emulate.

Recommendation: The UK Government should pursue a **single competent authority model** aimed at centralising information, skills and resources. BSA believes the **NCSC is best fit to assume this role.**

2. Security Requirements for DSPs

BSA welcomes the intention of the UK Government to take a "*guidance and principles based approach*" to the security requirements for DSPs. As the UK Government further develops the provision of security elements pursuant to Article 16(1) of the Directive, we recommend a **clarification that none of the suggested elements are binding in nature.** DSPs should be provided a level of flexibility when putting in place their baseline security measures. A direct obligation to include any of the measures and elements set out in the European Commission's future "Implementing Act" ("IA") would not respect the "*light touch*" approach of the Directive.

As the UK Government assesses the recently published European Commission draft IA, we wish to express our concern that while the draft states that "*DSPs remain free to implement security baseline measures as they see fit*", the draft remains fairly detailed on the question of what type of security baselines DSPs should seek to follow in order to be compliant with the requirements of the Directive. While many of the measures in the draft IA are directly drawn from ISO 27001, we would encourage the UK Government to **recognise that the NIST "Framework for Improving Critical Infrastructure Cybersecurity" and "UK Cyber Essentials" are also examples of best practice that would demonstrate compliance with the Directive.**

Regarding documentation, BSA is concerned with the approach taken by the European Commission, which would obligate all DSPs to fully document their security baselines and processes. Such an obligation would not correspond with the "*light touch*" regime of the Directive. It should remain up to each organisation how they prove they comply with the required security baseline measures. We encourage the UK Government to work with the European Commission to **change the wording in the draft IA from "*shall*" to "*should*".**

Recommendation: The UK implementation of the Directive should include a **clarification that the suggested security elements are voluntary** and that DSPs should have flexibility with respect to the implementation of baseline measures. The UK Government should also recognise that along with measures drawn on ISO 27001, the baselines set out in NIST's "Framework for Improving Critical Infrastructure Cybersecurity" and "UK Cyber Essentials" would **equally demonstrate compliance**. Furthermore, a clarification to the European Commission draft IA should be made so that DSPs are **not obliged to fully document their security baselines and processes**.

3. Incident Reporting for DSPs

BSA welcomes the recognition by the UK Government that incident reporting can be complex and challenging for organisations. Consequently, we encourage the UK Government to develop its incident reporting threshold around the **principle of availability and refrain from referencing integrity and confidentiality.** The NIS Directive focuses primarily on the availability of a service and does not refer to the latter two categories. BSA calls on the UK Government to respect the letter and spirit of the Directive and not seek to introduce additional requirements. The focus on incident reporting should instead be on the "continuity" of the service.

When considering the European Commission draft IA, BSA is concerned by its **overly prescriptive parameters for triggering the notification of incidents pursuant to Article 16(4).** The introduction of low thresholds (e.g. 5 million user hours) risks the possibility of over-reporting by DSPs and runs counter to the intention of the Directive. Numerical thresholds will also risk creating a "one-size-fits-all" incident reporting regime, which would not be appropriate as every incident needs to be properly analysed based on the merits of the incident. For many DSPs, it remains difficult to effectively calculate the total number of users affected by a cyber incident. For example, cloud computing service providers rarely have visibility beyond the "first layer" of customers, making it often impossible to calculate the total number of "users" impacted by an incident. In addition, the draft IA includes a geographic threshold which would prove to be unworkable as most DSPs tend to track incidents by regional data centres, not by political boundaries. BSA calls on the UK Government to work with the European Commission for further simplification of the incident reporting parameters in the final negotiation of the IA.

Furthermore, the UK implementation of the Directive should **avoid double reporting obligations and clarify the NCSC as the competent authority for DSPs**. A clear framework for liability and responsibility of incident reporting that would centre around one competent authority would provide much needed clarity.

Recommendation: Incident reporting should focus on the principle of **availability** and refrain from referencing integrity and confidentiality. The UK Government should work with the European Commission to **simplify the incident reporting parameters** set out in the draft IA and avoid the introduction of arbitrary quantitative thresholds. Double reporting obligations between the NSCS and the competent authority should be avoided and we reiterate the importance of setting up a single competent authority.

4. Penalties Regime

BSA takes note of the UK Government's proposal to align the penalties applicable to infringements of the Directive with the framework set out in the General Data Protection Regulation ("GDPR"). While the loss of an "essential service" could have a significant economic or social impact on a given industry or region, BSA believes that **penalties of up to 4% of global turnover are likely to be disproportionate** to the impact of an incident and will not lead to greater network and information security.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

The sanctions regime of the GDPR was set up to address an intentional or negligent gross failure to comply with the legislation. The GDPR specifically calls out cases where failure to comply would trigger such fines. **No such criteria exist for failure to comply with the NIS Directive**. If the UK Government chooses to pursue a penalties regime with fines of up to 4% of global turnover, a clear list of incidents that could qualify as necessitating such high fines would need to be created. BSA also calls on the UK Government to ensure that the future penalties regime reflects the Directive that in the case of an incident, "*notification shall not make the notifying party subject to increased liability*."

Furthermore, if the ICO is chosen as the competent authority for DSPs, BSA calls on the UK Government to **exclude with certainty the threat of "double fining"** under the GDPR and Directive. As the GDPR assumes *lex specialis*, any penalties related to the same data breach should be dealt with under the GDPR.

Recommendation: The proposed penalties regime should be revisited and developed as **administrative fines,** in line with other consumer protection penalties regimes. The UK Government should also see to re-assure businesses that it will **not seek to fine entities under both the GDPR and Directive for the same incident.**

For further information, please contact:
Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.1315