Brussels, 27 April 2018

BSA | The Software Alliance's feedback on the UK Government Targeted Consultation on Digital Service Providers

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") targeted consultation on how the Network and Information Security ("NIS") Directive will apply to Digital Service Providers ("DSPs").

As noted in our September 2017 consultation response, 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 NIS Directive will continue to apply in the UK. As the UK Government works to implement the NIS Directive as it applies to DSPs, we wish to provide the following comments:

1. **Competent Authority Framework** – The UK Government should consider pursuing a single competent authority model based around an authority most suited to assist and improve the network and information security of organisations across the economy.

2. **Identification of DSPs** – The UK Government should publish guidance to further guide entities in understanding whether they fall within the scope of the Directive in particular with regard to cloud services.

3. **Registration** – The UK Government should pursue a voluntary registration model focused on those DSPs which have their main establishment within the UK.

4. **Security Elements** – The UK Government should publish guidance clarifying that measures drawn from ISO 27001, 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 "Ten-Steps to Cyber Security" framework would demonstrate compliance with the Directive

5. **Incident Reporting Parameters** – The UK Government should publish guidance clarifying its interpretation of the thresholds set out in the European Commission Implementing Act ("IA") for DSPs with a particular focus on the calculation of affected

[1] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With offices in Brussels, 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, Box, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Intuit, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend 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

user hours, estimation of material damage, and measuring of geographical spread of an incident.

6. **Risk of Double Reporting** – The UK Government should publish guidance to aid DSPs in understanding which types of incidents should be treated as a NIS incident and which should fall under the General Data Protection Regulation ("GDPR") data breach notification framework. The guidance should also include further information on reporting for instances when a DSP is also classified as an Operator of Essential Services ("OES") to ensure that reporting to only the OES competent authority occurs.

7. **Costs** – The UK Government should place a strict cap on the fee it can levy on DSPs when recovering the cost of enforcing the Directive. Further clarity on the legal basis used to potentially levy an annual fee on DSPs should be provided while ensuring that any such fee is limited to DSPs who have the UK as their main establishment.

Issues and BSA Positions

1. Competent Authority Framework

BSA takes note of the UK Government's decision to move forward with a multiple competent authority approach while also designating the Information Commissioner's Office ("ICO") as the competent authority for DSPs. We continue to believe that **establishing a single competent authority is the preferred model** to allow for a consolidated centre of information with expertise across industry sectors.

Cross-industry expertise is important as cyber-attacks occur across sectors while adapting from the successes and failures of past intrusions. A regulatory model whereby each industry sector reports incidents to different competent authority's risks being ineffective as **information sharing will likely not occur in a timely enough manner.** As many multi-sector cyber-attacks often follow a pattern, it will be difficult to decipher its development if all information is not centralised with one competent authority. We continue to question whether separate sectoral competent authorities will all be able to reach the appropriate level of skills and expertise needed to handle incidents and effectively share threat information to ensure detection and deterrence across the entire UK economy.

Furthermore, we once again wish to **voice our concern with the designation of the ICO as the competent authority for DSPs**. Member States should seek to designate the competent authority with the highest level of expertise in the field of cybersecurity. While the ICO is well respected within the field of data protection, it has little experience in aiding organisation in detecting, deterring and defending against cyber-attacks.

Should the ICO rather than the National Cyber Security Centre ("NCSC") remain as the competent authority for DSPs, we would welcome the publication of guidance, as noted in the January 2018 UK Government's response to the public consultation ("Government consultation

response")[2], on how competent authorities will interact with each other and across other regimes such as the GDPR. Furthermore, in this situation, we would also welcome the publication of guidance from the NSCS setting out the level of support they intend to provide to other competent authorities together with the assessment tools to be used by competent authorities.

2. Identification of DSPs

BSA recognises the challenge faced by the UK Government in defining DSPs in a manner that is both compatible with the Directive and clear to all impacted entities. We therefore welcome the intention of the UK Government to fully respect the "light-touch approach" as highlighted in the Government's consultation response where it noted that "*the Government's intention has always been to … limit the scope of those who have to comply with the Directive to those companies whose loss of service could have the greatest impact on the UK economy either directly or through impact on other companies.*"

BSA believes that the additional definition clarifications provided by the Government are beneficial and will not only aid entities in assessing whether they will fall within the scope of the Directive but will also ensure that the UK's implementation of the Directive focuses on those organisations whose loss of service could have a significant impact on the UK economy.

Regarding the clarification of cloud computing set out in the Governments consultation response, BSA notes the UK Government has **focused on DSPs that provide public cloud services**. The UK approach significantly departs from the NIS Directive, which does not create a distinction between cloud services deployment models. We would welcome further clarification from the UK Government on the basis for such a distinction.

3. Registration

BSA views that the creation of a system for UK DSPs to proactively register with the competent authority as a **positive step in building a strong working relationship** between entities who fall within the scope the legislation and the regulator. The building of mutual trust between the competent authority and UK DSPs will be integral to ensuring cyber resilience.

We believe that any future registry should be **voluntary rather than mandatory** in full respect of the "one-stop-shop" principle, which is a critical element of the "light-touch approach" of the Directive. Any mandatory registration requirements should be limited to those DSPs who have the UK as their main establishment. All DSPs whose main establishment falls outside of the UK should be exempt from any mandatory registration. Furthermore, it remains unclear as to the **level of penalties an entity would face should it fail to register with the competent authority.** Further clarity on these issues is encouraged.

[2] *Government response to the public consultation – Security of Network and Information Systems, UK Department for Digital, Culture, Media and Sport (January 2018)*

4. Security Elements

BSA welcomes the recognition by the UK Government that DSPs are not required to meet the security requirements that were set out in the 2017 public consultation, which only apply to OESs. As the UK Government continues to assess the European Commission's IA for DSPs, we believe that any future guidance should **re-emphasise that DSPs remain free to implement security baselines measures as they see fit so long as they provide for adequate and sufficient security.** We also would welcome a reference to "state of the art" security similar to that which is found in Article 32(1) of the GDPR.

Furthermore, we would welcome additional clarity in the future guidance on the **types of security measures that the competent authority would view as sufficient**. We encourage the guidance to reference ISO 27001, the NIST "Framework for Improving Critical Infrastructure Cybersecurity," and the "NCSC Ten-Steps to Cyber Security" as examples of best practice that would demonstrate compliance with the Directive.

5. Incident Reporting Parameters

While BSA understands that the incident reporting parameters set out in the European Commission's IA are specific and the UK is bound by them, we believe that DSPs would benefit from additional guidance on how the competent authority interprets the provisions.

When considering the IA's Article 4(1)(a), we note that it will be **difficult for many cloud service providers to effectively calculate the number of "affected user hours" during an incident** as cloud service providers only have visibility of the "first-layer" of customers with whom they have concluded a contract. The determination of "5 million user hours" as set out in Article 4(1)(a) may be possible for those DSPs that can effectively measure the affected natural and legal persons with whom a contract for the provision of a service have been concluded. However, for many DSPs, they will be unable to make a proper determination of "5 million user hours" as they do not have a contractual relationship with all potentially affected users. Future guidance which clarifies how DSPs with no visibility beyond the "first-layer" can effectively measure "affected user hours" would be welcomed.

With regard to the IA's Article 4(1)(d), **estimating the material damage of a particular user** will be challenging for a DSP outside of a DSPs standard terms of use. We believe future guidance should address this issue and clarify that this only extends to any material damage which the DSP can reasonably assess within its existing practices.

Furthermore, the issue of **measuring the geographical spread of an incident remains troubling** for BSA members. As stressed in our 2017 consultation response, DSPs tend to track incidents by regional data centres, not by political boundaries. Anything impacting two customers located in two different Member States would, by definition, be "substantial." Due to the risk of overreporting, we would welcome additional guidance on how the competent authority will address the issue of geographical spread. We encourage the competent authority to interpret

this provision as f**ocusing only on a substantial area of customers within a given EU territory rather than focusing on cross-border incidents.**

6. Risk of Double Reporting

As highlighted above, BSA remains concerned that the designation of the ICO as the UK competent authority for DSPs **risks creating double-reporting for entities under the GDPR and NIS Directive**. While some significant incidents under the NIS Directive will also be classified as data breaches under the GDPR, there are certain instances where a NIS incident has occurred but a GDPR data breach has not. DSPs, particularly smaller entities, will likely struggle to differentiate between the two reporting frameworks leading to over reporting to the ICO. We encourage the drafting of **additional guidance to aid DSPs** in understanding which types of incidents should be treated as a NIS incident and which should be considered a GDPR data breach. For those instances where both occur as the result of the same incident, a **streamlined reporting procedure should be created**.

With regard to instances where a **DSP is also classified as an OES**, we believe that further clarity from the UK Government on incident reporting is necessary. While we welcome the acknowledgement that an agreement between the two competent authorities should be arranged so that only one notification is required, we believe that this framework should be clearly set out by the UK Government and not left open-ended. We believe that in **instances where an entity is both a DSP and OES, incident reporting should occur only with the OES competent authority**. It should then be for the OES competent authority to liaise with the DSP competent authority for any further actions.

7. Costs

We believe that further clarity is required on the UK Governments plans related to the costs of enforcement. While seeking to provide all competent authorities with the power to recover the costs of enforcing the Directive is understandable, we encourage the **introduction of a cap** to any such fee. This would ensure that any auditing costs born by the competent authority (or third-parties contracted by the competent authority) are kept within reason.

Lastly, we question the potential decision of the DSP competent authority to **levy an annual fee on DSPs**, in addition to recovering direct costs involved in any regulatory investigations. There is no basis within the NIS Directive for the levying of an annual fee, nor does such a provision exist within the GDPR. Further evidence of a legal basis to levy such a fee should be required.

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