Brussels, 11 October 2017

BSA feedback on European Commission's Network and Information Security Directive draft Implementing Regulation

BSA | The Software Alliance ("BSA")[i], the leading advocate for the global software industry, welcomes the opportunity to comment on the European Commission's draft Implementing Regulation ("IR") laying down rules for the application of Directive (EU) 2016/1148 with regards to security and incident notification requirements for digital service providers ("DSPs"). As the European Commission continues to refine its future secondary legislation, we wish to provide the following comments:

Light touch approach

It is important that the future IR respects the "light touch" approach for DSPs that is reflected in the Directive. BSA therefore welcomes the clarifications in Recitals 1 and 2 of the draft IR, which acknowledge that *"…digital service providers remain free to take technical and organisational measures they consider appropriate and proportionate…*" and when identifying such measures *"…digital service providers should approach information security in a systematic way, using a risk-based approach.*" We also welcome the recognition of the principle of data minimisation as set out in Recital 8.

Article 2 – Security elements

With regard to "Article 2 – Security Elements", we caution the European Commission against the introduction of a mandatory documentation requirement (Article 2(6)). Such an obligation would run counter to the "light touch" approach and does not reflect the requirements of the Directive as ex-ante audits are not required for DSPs. As entities may choose to utilise third-party auditors to comply with Article 16(1)(d) of the Directive, DSPs should be provided with additional flexibility to demonstrate compliance using any suitable means in consideration of the risk and costs involved. They should be encouraged, but not strictly required to produce documentation. We would also welcome additional clarity on Article 2(1)(b) as to how far back organisations would need to trace the critical supplies used in the provision of a service.

BSA supports the recognition in Article 2(5) that international standards relevant to the security of network and information systems may be used to comply with the Directive. However, to avoid market fragmentation through divergent standard compliance requirements, we would encourage the European Commission to explicitly reference frameworks such as ISO 27001 and the "Framework for Improving Critical Infrastructure Cybersecurity" issued by the U.S. National Institute for Standards and Technology ("NIST") as examples of internationally recognised frameworks.

As the European Commission further refines the security elements set out in Article 2 of the draft IR, we believe the final IR would benefit from additional clarity. While the security elements should

Avenue des Arts 44
1040 Brussels
Belgium

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

have definitional character, we encourage the European Commission to clarify that they are not binding requirements on DSPs. Although we welcome that many of the measures in the draft IR are directly drawn from ISO 27001, a direct obligation to include all elements set out in Article 2 would not respect the "light touch" approach of the Directive and exceed its stated policy objective which is the "continuity" of services. DSPs should be provided with a certain level of flexibility when putting in place their baseline security measures.

Article 3 – Parameters to be taken into account to determine whether the impact of an incident is substantial

With respect to "Article 3 – Parameters to be taken into account to determine whether the impact of an incident is substantial", BSA encourages the European Commission to reaffirm in the final IR that the focus of incident reporting should be on the "continuity" of the service as outlined in Article 16(2) of the Directive. BSA cautions against the introduction of "confidentiality" and "integrity" in Article 3(2) and Article 3(4) as these aspects are both sufficiently covered by the General Data Protection Regulation ("GDPR"). The Directive should seek to ensure that DSPs only report "significant incidents" while avoiding the creation of reporting overlaps with other legislation. The inclusion of "confidentiality" and "integrity" risks creating a regime where a DSP acting as a "data processor" will report an incident under the Directive before a "data controller" can notify the GDPR competent authority.

Moreover, BSA is concerned that assessing the impact on economic and social activities for potentially thousands of users (Article 3(5)) may prove to be difficult for most DSPs. We encourage the European Commission to focus such an assessment strictly on the entities under direct contract with the DSP.

Article 4 – Substantial impact of an incident

When considering "Article 4 – Substantial impact of an incident", we stress that incident reporting should focus on those incidents which are truly "significant" so that both DSPs and competent authorities are not overburdened with the reporting of minor incidents. To achieve this objective, the future IR should avoid being overly prescriptive and we caution against the introduction of low quantitative thresholds.

BSA questions whether the thresholds proposed in the draft IR, specifically Article 4(1)(a), would achieve the stated objective of the Directive that only "significant incidents" are reported to the competent authority. BSA interprets a threshold of 5 million user hours to equate to a 1-hour loss of service for 83,300 users. The significance of such a loss of service will likely depend on the number of users serviced by a DSP. If the DSP has a small number of users, this may be significant. However, if the DSP has millions of users, a 1-hour loss of service for 83,300 users will likely not represent a "significant incident" and risks creating an environment of over-reporting. Overall, such a threshold takes little account of the actual severity of the interruption of the service. A percentage of active licensed users impacted (e.g. 40%) may be a better approach. Numerical thresholds further risk creating a "one-size-fits-all" reporting regime, which

Avenue des Arts 44
1040 Brussels
Belgium

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

would not be appropriate as every incident should be properly assessed based on the risk posed by the incident.

When evaluating any future quantitative thresholds, BSA wishes to reiterate to the European Commission that for many DSPs, it remains difficult to effectively calculate the total number of users impacted by an incident. For example, cloud 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 and its corresponding financial impact. We encourage the European Commission to acknowledge this reality in its future IR.

Furthermore, with regard to Article 4(1)(e), BSA cautions against the introduction of a geographical threshold into the final IR. DSPs typically track incidents based on the area covered by a given data centre rather than by national jurisdictional boundaries. An exact determination of impacted jurisdictions is often difficult as many users access services via remote gateways, extraterritorial virtual private networks and other proxies that may be difficult to geo-locate, either for technical reasons or, more importantly, due to privacy law prohibitions. Moreover, even if such a determination could be made, the proposed threshold would mean that any incident affecting one or more users in two or more Member States would constitute a reportable incident. This will likely not constitute a "significant incident" for most DSPs.

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

[i] *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.