BSA's response to the Evaluation Roadmap/ Inception Impact Assessment on the NIS Directive review

Brussels, 13 August 2020

BSA | The Software Alliance (BSA) welcomes the opportunity to provide input to the Commission's evaluation roadmap/ Inception Impact Assessment on the NIS Directive. BSA is the leading advocate for the global software industry. Our members are at the forefront of software-enabled innovation that is fueling global economic growth by helping enterprises in every sector of the economy operate more efficiently.

BSA supports the development of relevant policy instruments and smart regulation that strengthen cybersecurity in Europe. In this respect, we acknowledge the positive role that the NIS directive has played in setting common minimum capabilities across the Union and the introduction of security requirements and of incident reporting procedures. Further harmonization of these elements should be considered in the review, accounting of the technological (i.e. the evolution of multi-cloud deployment) and legal (i.e. contractual obligations of technology providers vis-à-vis their regulated customers) evolutions. The general spirit of the existing provisions should be kept, but with a better level of harmonization and implementation, in particular with regard to service definitions, thresholds, reporting modalities, and on the categories of (sub)sectors recognised as OESs and DSPs across the Union.

In accordance with the current requirements, the provisions for operators of essential services (OESs) and digital service providers (DSPs) should remain risk proportionate and the differentiation between the requirements for critical operators, whose disruption could lead to a significant economic and/ or societal impact, and the more flexible approach that applies to DSPs, should be upheld. This model has demonstrated its efficiency as it not only helps Member States to naturally triage their incident response when assisting affected organisations, it also helps OESs as their incident reporting is being handled appropriately. Ultimately, this approach lowers reporting congestions and strengthens the overall resilience of the critical infrastructures. As an example, the COVID-19 outbreak has shown the importance of prioritizing sector-specific requirements for the segments that are critical to society. Notwithstanding the above, we believe that for cases where a provider is considered as both a DSP and an OES, further clarity should be provided as to its status and responsibilities at Union level. Finally, a special attention should be paid to the architectural specificities of some services or sectors, which could face additional reporting complexity, e.g. due to the cross-border nature of these operators.

If the scope were to be expanded to additional sectors, this would require extensive research, supported by empirical data and evidence and input from the security community. Addressing the disparities related to the types of (sub)sectors recognised as OESs or DSPs across the EU would help achieve a better level of harmonisation. With regards the call to expand the scope to software products, we would also like to underline that the sector is already covered within the Cloud services' inclusion in Annex III, notably through the Software As A Service principle. For the very limited cases where a software would not be delivered or serviced through the cloud (i.e. when embedded), the incident reporting obligations would be irrelevant, as the manufacturer would not have the visibility of the incident affecting that specific piece of software.

In addition, we believe that liability exemptions or safe harbours for reporting incidents are necessary and should be maintained in consistency with Articles 14(3) and 16(3) of the NIS Directive. Additional considerations include the necessity to provide clearer information to OESs and DSPs, including a one-stop-shop portal for information which can be useful when providers are cross-border in nature, and a stronger industry role with the NIS Cooperation Group and CSIRT Network.