AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

Response to the European Commission Consultation on the Draft Implementing Regulation on Digital Services Providers as foreseen in Article 16(8) of the NIS Directive

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2016, directly supports more than 4.5 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Summary (for website form)

To avoid market fragmentation through nationally divergent standard compliance requirements, the implementing measure should explicitly reference ISO27001/27002, the NIST Cybersecurity Framework - which is rapidly becoming a global best practice - or similar, and internationally recognised frameworks which Digital Service Providers (DSPs) can certify against.

To preserve the light-touch approach for DSPs and to avoid disproportionate intrusion in DSPs' normal business processes, the implementing measure should remain high-level in terms of the security outcomes to achieve.

To ensure that incident reporting stays focused on the most important cases, the thresholds proposed in Article 4 should be improved:

- The '5m user hours' threshold for 'availability incidents' would only work for those services where the term 'user' rests on the estimation of 'affected natural and legal persons with whom a contract for the provision of the service has been concluded' (Article 3(a)).
- For availability incidents (Article 4(a)) this parameter should not include planned maintenance or scheduled patches/updates to a digital service.
- Additional guidance would be helpful to clarify that continuity incidents which a DSP should report to an Operator of Essential Services under Article 16(5) of the NIS Directive should not count towards the threshold for the DSP's own notification obligation under Article 16(3).
- The determination of the geographical spread of incidents as required by the proposed Article 3(3) as well as the threshold proposed in Article 4(1)(e) would be uneasy, often inaccurate and in some cases even impossible for DSPs to do.

Moreover, in many cases it may not always be possible or it may take time for the DSP to gather the required information. Clarification on the format and processes for notification would be welcome, particularly where there are multiple players in a supply chain, in advance of the transposition date.

Finally, in the interest of the Digital Single Market, the one-stop-shop approach adopted for DSPs and Article 18(1) of the Directive should be explicitly referenced. The implementing regulation should allow DSPs to self-identify to the supervisory authority in the relevant Member State where their 'head office' is located, and a dedicated provision should clarify that DSPs are only required to report incidents to the authority they have identified as competent in the meaning of Article 18(1).

Detailed Consultation Response

The NIS Directive must be implemented so as to ensure the smooth functioning of the Digital Single Market and the achievement of positive outcomes for all, including service providers, service users, and national authorities. AmCham EU suggests the following:

To avoid market fragmentation through nationally divergent standard compliance requirements, the implementing measure should explicitly reference ISO27001/27002, the NIST Cybersecurity Framework - which is rapidly becoming a global best practice - or similar, internationally recognised frameworks which Digital Service Providers (DSPs) can certify against, and use that certification to demonstrate compliance both towards supervisory authorities and towards their own customers. While recognising that Article 19(2) of the NIS Directive provides for ENISA, in collaboration with Member States, to draw up advice and guidelines on standards, such guidance may not be available in due time to enable DSPs to certify against identified standards, where they are not already certified, and in advance of the May 2018 transposition date.

To preserve the light-touch approach for DSPs and to avoid disproportionate intrusion in DSPs' normal business processes, the implementing measure should remain high-level in terms of the security outcomes to achieve. The requirements proposed in Article 2 appear overly detailed and go well beyond the policy objective defined in Article 16 of the Directive which is to ensure the continuity of services in scope. Moreover, the requirement of Article 2(6) to comprehensively document every baseline adopted and every measure taken seems unnecessarily burdensome especially for smaller DSPs. As a principle DSPs should be allowed to demonstrate compliance using any suitable means in consideration of the risk and costs involved. They should therefore be encouraged but not strictly required to produce documentation on the top of taking effective security measures.

To ensure that incident reporting stays focused on the most important cases and that neither DSPs, nor supervisory authorities are overburdened with the reporting of minor incidents, the thresholds proposed in Article 4 should be reconsidered and possibly further simplified.

- The '5m user hours' threshold for 'availability incidents' may seem reasonable for services where the term 'user' rests on the estimation of 'affected natural and legal persons with whom a contract for the provision of the service has been concluded' (Article 3(a)); the same threshold, however, is particularly low for other services where no contract has been concluded and the service would be required to 'estimate the number of users having used the service based in particular on previous traffic data' (Article 3(b)). To put it in perspective: a non-critical fifteen-minute outage of an online search engine used during business hours by no more than 8-10% of the EU 28's active population would assuredly hit that threshold while, in reality, it would be unlikely to cause any more serious damage than momentary inconvenience for the average duration of a coffee break.

- One additional important consideration for availability incidents (Article 4(a)) is the clarification that this parameter does not include/apply to impacts on availability that are caused by planned maintenance or scheduled patches/updates to a digital service.

- Additional guidance would also be helpful to clarify that continuity incidents which a DSP should report to an Operator of Essential Services under Article 16(5) of the NIS Directive should not count towards the threshold for the DSP's own notification obligation under Article 16(3).

- The determination of the geographical spread of incidents as required by the proposed Article 3(3) as well as the threshold proposed in Article 4(1)(e) would be uneasy, often inaccurate and in some cases even impossible for DSPs to do. DSPs typically track incidents per data center coverage areas rather than by national jurisdictional boundaries. Rough estimates and indications may be possible to give, but the exact determination of impacted jurisdictions is all the more difficult that many users will access online service via remote gateways, extraterritorial virtual private networks and other proxies that may be difficult to geo-locate, whether for technical reasons or, more importantly, because of privacy law prohibitions to do so.

Moreover, given that Article 16(4) of the NIS Directive shall only apply 'where the digital service provider has access to the information needed to assess the impact of an incident against the parameters' [set out in Article 3 of the Implementing Regulation], it may not be possible or may take some time for the DSP to gather the required information. It is therefore also important that DSPs have clarification on the format and processes for notification, particularly where there are multiple players in a supply chain, in advance of the transposition date and taking account the practicalities identified above. This should be done either in this Implementing Regulation or in a subsequent implementing regulation, as provided for in Article 16(9) of the Directive.

Finally, in the interest of the Digital Single Market, the one-stop-shop approach adopted for DSPs and which Article 18(1) of the Directive centres on the main establishment of DSPs or on their EU representative should be explicitly referenced in the implementing regulation. Provision should be made in the regulation for DSPs to self-identify to the supervisory authority in the relevant Member State where their 'head office' is located. This is particularly important for companies with multiple establishments across the EU so that they can demonstrate compliance to authorities and their customers. Guidance on what is deemed to be a 'head office' for companies that are established in multiple member states would be helpful. Lastly, a dedicated provision should clarify that DSPs are not required to report incidents in multiple Member States but should report them to the authority they have identified as competent in the meaning of Article 18(1), on the understanding that, as per Article 17(3), supervisory authorities will cooperate across borders where appropriate.