Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845

Deloitte EU Policy Centre
Rond-point Robert Schumann 11
1040 Brussels
Belgium
+32 (0)2 600 68 25
www.deloitte.com

European Commission
Directorate-General for Communications Networks, Content and Technology
Unit H.2
For the attention of Mr Jakub Boratynski
1049 Brussels
Belgium

Brussels, 2 October 2020

Dear Sir/Madam,

European Commission public consultation on the revision of the NIS Directive

On behalf of the Deloitte[1] firms in the EU, and in addition to our response to the Consultation on the Directive on Security of Network and Information Systems ("NIS Directive"), we would like to highlight a few key messages for your consideration.

The NIS Directive has fostered cyber resilience in the EU, by increasing capabilities, preparedness, cooperation, information exchange, and awareness in the field of Network and Information Security. In the context of the increasing interdependence of the Digital Single Market with technological advances, Deloitte welcomes the European Commission's decision to anticipate the review of the Directive. Deloitte supports the efforts of the Commission to evaluate the objective of the NIS to increase the overall resilience of the Digital Single Market, by promoting joint action at the Union level. To respond to the consultation, Deloitte leveraged its network offering professional services to actors impacted by the adoption of the NIS Directive.

Increased efforts will be required to establish homogenous definitions of cybersecurity requirements to enable effective cooperation between states and industries at an international level. For instance, we underline the importance of making explicit reference to pre-existing common standards (i.e. ISO 27001, NIST), agreed regulatory requirements of specific industries and voluntary industry practices in the revision of the NIS Directive. This could potentially contribute to the creation of common and possibly binding cybersecurity standards at the international level, while also considerably sharpening and strengthening cooperation and joint response capabilities.

In the context of the upcoming review of the NIS Directive, we encourage the European Commission to promote targeted changes to clarify the NIS Directive, taking into account the following aspects:

[1] https://www2.deloitte.com/dl/en/legal/about-deloitte.html

- The entry into force of the NIS Directive in May 2018 is still too recent to have produced a measurable impact: most Member States have only recently implemented the changes brought about by its provisions;
- The level of information sharing on the NIS implementation is still limited and fragmented;
- The COVID-19 crisis has accelerated the pace of digitisation, increasing the growing dependence of essential services on ICT and proving to be a catalyst for cybercriminals all over the world.

Risk-based approach

- We encourage the Commission, Member States, and all actors identified under the NIS Directive, to adopt a risk-based approach to address cyber risks.
- We invite the Commission to raise awareness about the importance of enterprise-wide cyber risk management among the entities' Board of Directors, in collaboration with designated National Authorities.

We emphasize the importance of the NIS Directive promoting a culture of risk management. Improving the level of cyber security across the Union cannot be achieved with a rules-based approach. Instead, Member States need to translate this paradigm change – from a compliance-based to a risk-based approach – into their national strategies and implementation guidelines. The European Commission can support this change in mindset and narrative, by continuing to define cyber risk frameworks for network and information security.

At the same time, companies should take measures involving risk assessment and the implementation of security measures appropriate to the risks faced. In that respect, we believe that resilience towards cyber risks should become a priority for the Board of Directors. Cyber and infrastructure security need to become strategic, rather than being treated as merely compliance issues.

Harmonisation

- We call on the Commission to strengthen its action to promote harmonisation, particularly for the Member States' identification of Operators of Essential Services (OES) and of information sharing practices.
- We recommend to the Commission to propose measures to encourage further harmonisation of security and incident notification requirements at the level of the European Union level, while respecting the principle of subsidiarity.

We support Member States' efforts to achieve a higher level of security of network and information systems since the entry into force of the NIS Directive in 2016. Member States have adopted or maintained minimum capabilities and a strategy ensuring a level of security and network information systems. This is an essential element to facilitate strategic cooperation between all Member States in the cyberspace.

However, companies in the Single Market are still operating in an uneven level playing field due to different security and incident notification requirements. In particular, governments have taken different approaches in the identification of OES resulting in inconsistencies across countries, as underlined by the Commission's Report assessing the consistency of the approaches in the identification of operators of essential services published in October 2019.[2] The current lack of harmonisation can be tempered with EU action focused on the use of primary

[2] https://ec.europa.eu/digital-single-market/en/news/report-assessing-consistency-approaches-identification-operators-essential-services

and secondary Union law and standards developed together with the European supervisory authorities and in respect of the subsidiarity principle.

Security requirements and Information sharing

- We endorse coordination between Member States on harmonising security requirements by sharing information and best practices within the Cooperation Group, the CSIRTs Network, and ENISA.
- We recommend that the Commission and the Cooperation Group work on streamlining basic security requirements as further guidance would be highly beneficial to reduce the current fragmentation and improve effectiveness in the long term.

We note with concern that the lack of information shared in the Cooperation Group has hindered its capacity to encourage harmonisation in the implementation of the Directive. Member States have taken different approaches when transposing the Directive and they have communicated limited information to the European Commission on the progress made. As a result, the Cooperation Group did not have enough information to promote cross-border identification of OES.

The EU can have a great impact by providing incentives to build trust among relevant stakeholders, possibly via directing resources under the Connecting Europe Facility and the upcoming Digital Europe Programme towards Cooperative Models for Public Private Partnership (PPPs) and Information Sharing and Analysis Centers (ISACs). ISACs have formed spontaneous forums of collaboration between companies, civil society and regulators, to develop publicly accessible information sharing environments, as well as perhaps relevant best practices collected and produced by relevant EU and Member State authorities and agencies.

Sectoral approach

- We support a risk-based approach for sector classification.
- We suggest that the EU proposes joint action only in sectors that are essential across all Member States, after setting up a benchmarking mechanism for OES between Member States.

The European Commission has already taken considerable steps in 2019 to assess the impact of the Directive on the infrastructure providing essential services to all European citizens. In the report assessing the consistency of approaches in the identification of OES, the Commission provides an overview of the methodologies adopted by Member States to identify OES. It is important to note that, due to the different identification methods, the number of identified services varies when looking at Member States as a whole but also when taking a closer look at sectors and subsectors. We expect more information on these consistency gaps in the upcoming impact assessment and evaluation report on the NIS Directive. We discourage the inclusion of more sectors and sub-sectors in Annex II of the Directive based on the information collected so far. Sectors' vulnerability significantly varies between Member States. Hence, adding specific sectors in the scope of the Directive should remain the responsibility of Member States.

Incident reporting requirements

- We suggest that regulators provide a common holistic procedure across the Union for OES to report incidents.

With respect to incident reporting, we note that companies and organisations need to comply with different regulatory frameworks, each setting their own rules with respect to thresholds, timeline for reporting and workflows, with different supervisory authorities. Some sectors have initiated cooperation to harmonise incident

reporting requirements (i.e. financial services sector) via platforms that anonymise and encrypt the information-shared while automatically re-directing the incident to the relevant authority.

Regulators should encourage those initiatives and take it even further by means of an adaptive approach. This approach relies on an iterative process of feedback loops, where outcomes can contribute to revisions of that regulation to help make it more effective. These feedback loops allow regulators to assess policies against set benchmarks, which then can be used as input for revisions. Regulators and businesses can use many tools to get such feedback, including setting up policy labs, creating regulatory sandboxes, crowdsourcing policymaking, and providing representation to industry in the governance process via self-regulatory and private standard-setting bodies.

Third-party providers

- We encourage the Commission to extend the scope of Digital Service Providers under the NIS Directive to Managed Security Services (MSS).

With respect to supply chain due diligence regarding cybersecurity, we acknowledge that companies increasingly opt to outsource services to third parties, bringing along important cybersecurity concerns. Cyber-attacks to the supply chain carry reputational and operational impact on the company and can endanger European citizens. Indeed, the current lack of security requirements for companies providing outsourced services can undermine even those companies that have strong cybersecurity strategies in place.

Ensuring cybersecurity of the supply chain must become a priority for the European Commission. It demands a common effort both on the physical and cyber security of assets and services along the system's lifecycle (feasibility, analysis, design, development, maintenance, etc.). Moreover, since there is no geographical limit to outsourcing, we strongly encourage the Commission to engage discussions at a global level, on the basis of global standards.

National Cyber Strategies

In terms of actors involved in the review of national cyber strategies, we propose the following governance framework:

- Governments should better clarify the responsibilities of the roles identified within their cyber governance framework on cybersecurity to avoid institutional conflict among the different ministries and institutions.
- Computer Emergency Response Teams should give guidance to those responsible for responding quickly to changes in the cyber threat situation and acting in the interests of anticipatory protection of their society and economy.
- ENISA should have more power and resources to facilitate the exchange of best practices on cyber capabilities.
- The Cooperation Group should act as the strategic layer of the discussion on cyber capabilities by promoting information-sharing between the NIS actors and national authorities.

Having regular reviews of national cybersecurity strategies remains a priority for Member States. Governments should thoroughly and regularly review strategies. In some cases, existing strategies may already adequately protect against the largest threats from a new technology. In other cases, new technology may change the underlying dynamics such that new elements must be included in national strategies – such as the normative

evolution of the international law of cyberspace. Trend and scenario analyses would appear to be suitable tools to predict the prevailing uncertainties in cyberspace and to respond to them. The perception of the threat situation and responsibility underlying the strategies could be reviewed at regular intervals or on a permanent basis. We believe that this will establish dynamic processes for adapting cybersecurity strategies.

Furthermore, we would like to draw your attention to the following Deloitte publications:

- *"Developing cybersecurity capabilities for the EU NIS Directive" assessing the results of a Survey dedicated to the NIS Actors (OES in particular):* https://www2.deloitte.com/be/en/pages/risk/articles/Developing-cybersecurity-capabilities-for-EU-NIS-Directive.html
- *European Cyber Defense – Part 1: Strategies: Status quo 2018:* https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Deloitte-European-Cyber-Defense-Report-Part-1.pdf
- *European Cyber Defense – Part 2: Strategies: Future of Cyber Security 2030* https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Deloitte-European-Cyber-Defense-Report-Part-2.pdf

And to the *Deloitte Cyber Security Framework*, which promotes a risk management approach to cyber-resilience: https://www2.deloitte.com/be/en/pages/risk/solutions/cyber-strategy-framework.html

If you have any questions concerning our comments, please contact:

Inge Bryan (ibryan@deloitte.nl), Andrea Rigoni (arigoni@deloitte.it), Jan Vanhaecht (jvanhaecht@deloitte.com) or Peter Wirnsperger (pwirnsperger@deloitte.de).

Yours sincerely,

Inge Bryan

Partner Deloitte Netherlands, Cyber Risk Services and Public Policy Leader

Andrea Rigoni

Partner Deloitte Italy, Global Government and Public Services Cyber Leader

Jan Vanhaecht

Partner Deloitte Belgium, Cyber Secure Domain Leader

Peter Wirnsperger

Partner Deloitte Germany, Public Sector Risk Lead