OPEN PUBLIC CONSULTATION ON THE DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS ('NIS DIRECTIVE')

Summary Report on the open public consultation on the Directive on security of network and information systems (NIS Directive)

Disclaimer: the views presented in this factual summary report are not the views of the European Commission but of the stakeholders that participated in this open public consultation.

TEASER: The public stakeholder consultation took place between 7 July and 2 October 2020. It was conducted to gather views on the topic of cybersecurity policy as well as on the different elements of the NIS Directive. The overall number of responses submitted was 206, and consisted of contributions from Member State competent authorities, EU bodies dealing with cybersecurity, operators of essential services, digital service providers, trade associations, researchers and academia, cybersecurity industry professionals, consumer organisations and citizens. The results of the consultation were used for the evaluation and impact assessment of the NIS Directive.

Objectives of the consultation

The open public consultation (OPC) aimed at collecting the views of Member States competent authorities, Union bodies dealing with cybersecurity, operators of essential services (OES), digital service providers (DSPs), as well as economic entities that could potentially become OES and DSPs in light of a revised NIS Directive, trade associations, researchers and academia, cybersecurity industry professionals, consumer organisations and citizens. All these different stakeholder groups have important information and insights on actions taken for the implementation of the NIS Directive, as well as interest in and opinions on shaping the debate about the possible options for the future.

The stakeholder consultation had two main objectives:

(1) collect views on the implementation of the NIS Directive (to support the analysis on the retrospective evaluation of the Directive)

(2) and collect views on the impacts of possible future changes to the legal act (to support the forward-looking assessment).

It posed general questions designed to collect feedback from the general public and more technical questions targeting expert stakeholders.

Who replied to the consultation?

The questionnaire was made available in all 24 official EU languages, ensuring that the public consultation was accessible to as many stakeholders as possible, especially citizens. 206 replies were collected online, of which 182 were replies provided by actors located in EU Member States. Respondents from Belgium were most numerous with 47 responses (22.8%), followed by 24 responses from Germany (11.7%), 18 responses from Austria (8.7%) and 17 responses from France (8.3%). Regarding countries outside the EU, 12 responses were received from the USA (5.8%).

Trade associations representing both sectors covered by the NIS Directive and sectors that do not fall within the scope of the NIS Directive make up a third of the sample (68 responses) closely followed by companies covered by the NIS Directive, i.e. operators of essential services and digital service providers (57 responses). Other stakeholders (36 responses) include economic operators not covered by the NIS Directive, consumer organisations and EU bodies. 14 responses were submitted by national competent authorities (CSIRTs included), while 10 responses were received from individual citizens.

Table 1 Respondent types in the sample

Type of organisation	No. of responses	% response
Trade associations	68	33.0%
OESs and DSPs*	57	27.7%
Other stakeholders	36	17.5%
Cybersecurity professionals	21	10.2%
NCAs and CSIRTs	14	6.8%
Citizens	10	4.9%
Total	206	100%

Source: OPC results
**44 OESs and 13 DSPs*

Findings of the open public consultation

Relevance of the NIS Directive

Respondents were asked to indicate the extent to which the **objectives of the NIS Directive are still relevant**. An overwhelming majority of the respondents indicated that the objectives of the Directive are still relevant, and even very relevant. To the respondents, the most relevant objective of the three is to promote a culture of security across all sectors vital for the EU economy and society (77.2%). Similar response patterns were observed across different respondent categories.

Cyber threat landscape

Respondents were asked for their views on the evolution of the cyber threat landscape since the entry into force of the NIS Directive. An overwhelming majority of respondents indicated that the **cyber threat level has increased since 2016 (88.4%)**, with 43.7% believing it has significantly increased. Across different respondent categories there is a consensus that the cyber threat level has increased since 2016. The respondents on average rated SMEs as rather poorly prepared in dealing with the evolving cybersecurity threats.

Responses suggest that an increase in cybersecurity risk can notably be observed in the health sector, digital infrastructure, banking, electricity and financial market infrastructures. At the same time, respondents indicated that banking and financial market infrastructures hold the highest level of cybersecurity resilience. Conversely, the level of preparedness of the health sector was found to be the lowest by respondents.

Added value of EU security rules

An overwhelming majority of the OPC respondents agreed that **common EU rules are needed to address cyber threats**. Two-thirds of them strongly agreed that cybersecurity rules should be aligned at EU level given that cyber risks can propagate across borders at high speed. Just over half (56.3%) of the OPC respondents strongly agreed with the statement that mandatory sharing of cyber-risk related information between national competent authorities across the EU would contribute to a high level of joint situational awareness on cyber risks.

Sectorial scope of the NIS Directive

Respondents were asked for their views about the appropriateness of the NIS Directive's sectoral coverage. The overall results revealed that OPC respondents on average show significantly more **support for the inclusion of public administrations and data centres within the scope of the NIS Directive**. Just over half of the respondents supported the coverage of the **chemicals** (51.4%) and **food supply** (50.5%) industries.

Cyber professionals were more likely to agree to extend the scope of the NIS Directive to include further sectors and types of digital services at risk of cyber threats. On the other hand, OESs, DSPs and trade associations were far less likely to agree with 22.8% and 25% of them respectively disagreeing with the prospect of including further digital services within the scope of the NIS Directive.

Overall, the most frequently mentioned sectors in the respective open field questions were (in order of importance):

- Public services – e-government, e-health, and emergency services (police, fire)
- Telecommunications
- Energy and electricity
- Cloud and DNS providers
- Manufacturers of electronic hardware and software
- Traditional media online
- Social media platforms
- Postal and courier services
- Data centres
- Banking, finance, and insurance
- Food production and waste management

When asked about digital service providers, the most reported types of services which respondents considered should be included in the NIS Directive were:

- Data centres
- Social media platforms (social networks)
- Manufacturers and suppliers of important hardware and software
- Providers of communication and navigation services
- Service hosting providers
- All digital or internet products and services
- Application service providers (SAAS) and stores
- Online collaboration environments/tools, including video conferencing
- ICT security services

- Outsourced services such as application maintenance, Third Applications Formula and testing: externalised management tests, and BPO: Business process Outsourcing
- OTT services
- Telecoms
- Managed service providers and Managed Security Services (MSS),
- Payment provider gateways and financial transactions sites

Regulatory treatment of OESs and DSPs

The respondents were asked to agree or not as to whether the "light-touch" regulatory approach applied towards DSPs is justified and therefore should be maintained. OPC respondents **more frequently believed that the "light-touch" regulatory approach applied to DSPs is no longer justified** and should not be maintained (39.8%) while almost of third of the respondents could not express an opinion on this issue. Conversely, only 27.7% of the OPC respondents thought the regulatory "light-touch" for DSPs should be maintained. Among the responding Digital Service Providers, however, 69.2% thought that the "light touch" regulatory approach should be maintained and only 23.1% that it should be done away with.

National competent authorities and CSIRTs

The respondents were asked to assess the extent to which the NIS Directive impacted national authorities dealing with the security of network and information systems. Specifically, the question covered the following five components: (i) level of funding; (ii) level of staffing; (iii) level of expertise; (iv) cooperation of authorities across Member States; (v) cooperation between national competent authorities within Member States.

Results suggest a strong perceived impact of the NIS Directive with about every second respondent indicating a medium to high effect across all five areas. The share of those choosing low impact ranges between 7.3% and 9.7%. In the meantime, the portion of those finding the NIS Directive had no impact remains marginal (1.0%-1.9%) regarding funding, staffing and expertise. No respondent chose this answer option when it comes to aspects of cooperation.

Responses indicate a relatively strong perceived impact of the NIS Directive on national CSIRTs across the Member States. Nearly every second respondent considered that the Directive had high or medium impact across the six areas covered. In this regard, there appears to be no major discrepancies in response patterns. The Directive is found to have had the strongest impact regarding cooperation with OES and DSP. The share of those stating no impact is marginal, accounting for 0.5-1.5% of all answers.

Identification of OESs and sector-specific aspects

The respondents were asked about the effectiveness of the OES identification process. A **significant share of respondents finds that the current approach does not ensure that all relevant OES are identified across the Union** (37.4% disagrees and 6.3% strongly disagrees). In the same vein, above 40% of respondents disagree or strongly disagree with the

statement that the identification process has contributed to the creation of a level playing field for companies from the same sector across the Member States.

On the other hand, it appears that there is a more positive view as for the active engagement of competent authorities with OES. Similarly, according to the majority of the respondents, OES are aware of their obligations under the NIS Directive.

A total of 115 OPC participants provided free-text answers. The most often discussed topic is the **lack of harmonised approach resulting in significant inconsistencies in the way that Member States draw up lists of OES**, divergent applications of the thresholds and different applications of the lex specialis principle. Companies of the same nature therefore might be imposed different requirements depending on the Member State where they operate. Likewise, a same company might be identified as OES in one Member State, a DSP in another Member State, or a service provider falling out of the NIS Directive in yet a different Member State. Existing convergence tools (i.e. Article 5(4) consultation procedure, and the NIS Cooperation Group working document on the identification of OES) have not been sufficiently used to achieve consistent identification of OES across the Union.

Analysing OPC responses concerning the scope of the NIS Directive related to essential services, the question of lowering identification thresholds appears to be most divisive with nearly equal share in favour and against.

The responses relating to the question of the identification of OESs point out that Member States' approaches often show strong heterogeneity. To that end, it was suggested to set a common set of criteria to ensure a harmonised process of identification of OES.

The NIS Directive gives a wide room of discretion to Member States when it comes to the identification of operators of essential services, the setting of security requirements and the rules governing incident notification. Most respondents agreed that the approach leads to significant differences in the application of the Directive and has a **strong negative impact on the level playing field for companies in the internal market** (40.3%); the approach increases costs for OES operating in more than one Member State (48.1%); and that the approach allows Member States to take into account national specificities (52.9%).

Responses related to the context of OES identification refer to the **need to cover the public sector** by the Directive considering the magnitude of data they treat and potential impacts of a cyberattack. These answers argue that every sector working with essential data like personal data or business data should be compliant with the NIS Directive. In particular, the public sector should be included in the scope of the Directive, and more specifically all emergency services (e.g. police, fire brigade, technical aid), public administrations (e.g. citizens' offices) as well as government offices at regional, state and federal level.

A handful of responses set out concrete (sub-)sectors to be covered by the NIS Directive. In light of the COVID-19 pandemic, the **pharmaceutica**l sector has been identified.

Additionally, a small share of OPC answers covered the **transport sector**. According to these, the **automobile industry** should be covered by the NIS Directive. Additionally, one

response notes that transport (including rail, air, water) should differentiate between freight (referring to it as critical) and passenger transport (referring to it as not critical). **Food supply** and **manufacturing** have also been mentioned by a few OPC participants.

SMEs

Responses suggest insufficient cyber resilience and risk management practices applied by SMEs. Particularly, **small companies appear to be most vulnerable** in this regard with 27% of respondents providing lowest-possible evaluation.

As far as small enterprises are concerned, 95 free-text answers have been received. Nearly all replies relate to the obstacles hindering their cybersecurity resilience. These argue that small companies often lack the financial and human capacity, staff and awareness to provide adequate cybersecurity to their operation. **A large share of small companies do not perceive cyber threats as a risk to them or find that they do not face the same level of risk presented by large or medium sized companies.** Answers note that the concern with a small company is when they have access into, or are connected with, larger targets, and thus become the vectors for cyber-attacks on more critical targets.

98 free-text answer have been received in relation to medium-sized companies. Issues discussed are strongly comparable to those mentioned in relation to small companies. These entities, although most often have some sort of cybersecurity strategy in place, lack sufficient capacity (technical, financial, and human) to develop cybersecurity capabilities matching increased threats and risks compared to those in relation to small enterprises.

There is an overall agreement that the level of resilience and risk management practices applied by SMEs differ from one sector to another. There appears to be an agreement that discrepancy exists related to level of resilience and the risk-management practices both by size of the enterprise and the (sub-) section in which it operates. These point out that in some sectors (i.e. banking, energy) there is a strong legislative framework and high level of cybersecurity maturity.

Many parties explained their lack of knowledge or opinion on whether the exclusion of micro- and small enterprises from the scope of the NIS framework would be just withtheir smaller impacts (38.8%). Objection to the statement came notably from cybersecurity professionals (of whom 42.9% disagreed or strongly disagreed with the sentiment), although this audience group in particular was starkly divided on the issue with almost half (47.6%) also taking the opposing stance. Trade associations and other stakeholders expressed greater support for the notion that micro-/small enterprise should be excluded from conventional treatment, however, with 42.6% and 30.6% of those asked agreeing or strongly agreeing, respectively.

Most of the OPC respondents (60.2%) either agreed or strongly agreed that European legislation should require Member States to put in place frameworks to raise awareness of cyber threats among SMEs and to support them in facing cyber threats. Only 5.8% of the respondents either disagreed or strongly disagreed.

The NIS Directive's light-touch approach vis-à-vis DSPs

Almost half (48.5%) of respondents asked about the effectiveness of the light-touch approach towards DSPs agreed that the **cross-border nature of the NIS Directive's operations justified the harmonised treatment of DSPs by comparison to OESs**. Much of the audience however (36.9%), expressed no overall stance on the matter. Amongst parties who objected most strongly to the statement that the approach was contextually justified were OESs and DSPs themselves (19.3% of whom disagreed or strongly disagreed), indicating that groups most affected by the approach may feel more negatively towards the NIS Directive's approach than those that are less impacted.

Opinions on whether national authorities' degree of supervision could be justified by the nature of services and cyber risk faced, in the case of DSPs, were divided. Over a third of respondents representing citizens (40.0%), cybersecurity professionals (42.9%) and national competent authorities (42.9%) disagreed or strongly disagreed with the statement, although among other groups, opinion was decidedly less negative. Trade association representatives, OESs and DSPs and other stakeholders generally perceived the justification of the level of national supervision to be more reasonable.

As regards the level of DSPs cyber resilience, overall, participants rated cloud computing services as being the most prepared when it comes to cybersecurity related risks (32.5% said high or very high), followed by online search engines (24.8%), and lastly online marketplaces (20.9%).

Security requirements

Most respondents thought that imposing **security requirements on OES** by the NIS Directive has high and medium impacts in terms of cyber resilience. This opinion was shared among all types of stakeholders, but especially among OESs & DSPs (43.9% and 36.8%) cybersecurity professionals (47.6% and 19%), and citizens (50% and 40%).

While respondents overall appreciate the security requirements brought by the NIS Directive, **lack of harmonisation limits its impact**. The impact might be lower for large organisations as there was already an incentive on companies to protect themselves. Impacts are different also across sectors and Member States. It was noted that most of the NIS requirements were already in place before NIS Directive, and adaptions had to be made on the incident reporting process.

Concerning the impact of imposing **security requirements on DSPs** by the NIS Directive, most stakeholders were not able to comment on the nature of the impact, including OESs & DSPs, Trade associations, NCAs & CSIRTs. However, those that did believed it had medium to high impact.

Overall, OPC respondents thought that DSPs addressed in the NIS Directive were already aware of cybersecurity and had reasonable cybersecurity measures in place to protect their business models. Given the light-touch regime prescribed by the NIS Directive towards DSPs, the imposition of these maximum security requirements currently has a minimal impact on

DSPs. The impact of imposing security requirements on DSPs also depends on the country. In countries where the maturity was initially low, the NIS had more impact.

Most stakeholders could not answer or disagreed with the statement that there is sufficient degree of alignment of security requirements for OES and DSPs in all Member States.

Respondents noted that while all Member States have introduced measures in accordance with the Directive so that OESs and DSPs have to have security requirements in place, improved alignment between the various approaches adopted in different Member States would be helpful because the wide discretion that is given to Member States under the NIS Directive with respect to identifying OESs and establishing security requirements leads to incongruity between the different Member States.

The stakeholders were asked a series of questions on the different approaches of Member States towards security requirements. Most respondents agreed that: prescriptive requirements leave too little flexibility to companies (49%); prescriptive requirements make it difficult to take into account technological progress, new approaches to doing cybersecurity and other developments (48.1%); the different level of prescriptiveness of requirements increases a regulatory burden for companies operating across different national markets (44.7%); the companies should have the possibility to use certification to demonstrate compliance with the NIS security requirements (45.6%). Some respondents noted that a higher level of prescription that is outcome-focused is required in order to create sufficient common understanding of what is the regulatory obligation, as well as in order to provide the necessary incentives to organizations to pursue that compliance.

Incident notification

Member States are required to ensure that entities notify the competent authority or the CSIRT of incidents having a significant impact on the continuity of services. Stakeholders were asked about the implementation of notification requirements under the NIS Directive. Most respondents agreed that: different reporting thresholds and deadlines across the EU create unnecessary compliance burden for OES (39.8%); Member States have imposed notification requirements obliging companies to report all significant incidents (43.2%); and that the majority of companies have developed a good understanding of what constitutes an incident that has to be reported under the NIS Directive (41.3%). On the other hand, more stakeholders did not know (39.8%) or disagreed (31.6%) with the statement that the current approach ensures that OES across the Union face sufficiently similar incident notification requirements.

Respondents noted that since there are sometimes large differences in the definition of mandatory reporting of security incidents in the Member States, there are also **no uniform reporting obligations**. The lack of harmonisation for reporting of security incident under various regulations and programs, e.g. PSD2, GDPR, NIS, has led to a fragmented approach and creates an unnecessary compliance burden for OES. The lack of harmonization of incident reporting requirements at EU level is suggested an important issue. Identifying the right authority to inform and the right information to provide appears to be a heavy burden for

firms along the critical path of managing the incident itself. Fragmented approaches across Member States are suggested to imply additional regulatory and compliance burdens on companies.

The responding OESs and DSPs were overwhelmingly against the broadening of reporting obligations under the NIS Directive. This is also the case among the responding trade associations representing sectors both covered and not covered by the NISD. National competent authorities and cybersecurity professionals remain split on the issue.

As the OPC respondents were asked to think about ways of improving the information available to cybersecurity authorities on national level, they were then asked to describe which information gathered by national authorities should be made available at EU level to improve common situational awareness. The most frequent information types given, in order of importance, were as follows:

- Aggregated statistical data describing the current cyber threat landscape.
- Top threats and top incidents in terms of occurrence.
- Emerging cyber threats.
- Incidents with cross-border relevance.
- Indicator of Compromise (IOC) notifications based on level of seriousness.
- Attacks on sectors, attack vectors, critical vulnerabilities.
- Best practices on risk identification, remediation and/or mitigation.

Information sharing

The respondents were asked to evaluate the level of incident-related information sharing between Member States. Setting aside those not in the position to reply, it appears that the level of information-sharing between Member States requires substantial improvement. A larger proportion of OPC respondents were critical than those assessing this aspect positively.

OPC respondents were also asked about ways in which organisations could be incentivised to share more information with cybersecurity authorities on a voluntary basis. The most frequent suggestions made by the respondents revolved around the simplification of reporting processes guaranteeing anonymity, as well as free and transparent access to anonymised reporting information.

The respondents were also asked to rate the level of information exchange on cybersecurity between organisations in their respective sectors. Around three-quarters of the respondents were unable to provide a rating. The level of information exchange was ranked the highest among organisations in the financial and banking sectors and the lowest among organisations in the health sector. A third of the respondents indicated a low level of information exchange across sectors, while a further 8.7% indicating a very low level. Just over a quarter of the respondents (26.7%) indicated a medium level of information exchange across sectors. Very few respondents thought the level of information exchange across sectors was high (3.4% or 7 out of 206 respondents).

The OPC respondents were then asked how the level of information exchange between companies could be improved within Member States but also across the European Union. The most frequent suggestions were made, in order of importance:

- Centralising the information sharing duties either at EU or national level.
- Greater role for CSIRTs: establishing trusted CSIRTs and encourage sectoral-level CSIRTs to foster national and international information-exchange.
- National boards of experts meeting regularly to exchange information and best practices on mitigation and remediation.
- Through structured and trust-based mechanisms ensuring anonymous information sharing by competent authorities.
- Developing European-level ISACs at sectoral level.
- Industry-led initiatives for intra-sector information sharing between OES.
- Making it a legal obligation through an EU-level regulatory activity.
- Promote the use of robust, automated information sharing architectures, capable of turning threat indicators into security protections in near-real time.

Enforcement

Most respondents did not know or were unable to answer whether: Member States are effectively enforcing the compliance of OES (45.1%); Member States are effectively enforcing the compliance of DSPs (62.1%); the types and levels of penalties set by Member States are effective, proportionate and dissuasive (50.5%); and whether there is a sufficient degree of alignment of penalty levels between the different Member States (63.6%).

Efficiency

Most stakeholders agreed to some extent that **the effects of the NIS Directive have been achieved at a reasonable cost**. In particular, trade associations (42.6%, plus 7.4% to a large extent), OESs & DSPs (40.4%, plus 17.5% to a large extent), NCAs & CSIRTs (35.7%, plus 14.3% to a large extent), cybersecurity professionals (38.1%, plus 9.5% to a large extent), and citizens (50%). The majority of stakeholders thought that the **NIS Directive had medium to high impact on the overall level of resilience against cyber-threats across the EU**. This opinion was shared especially among the OES & DSPs (33.3% high impact and 38.6% medium impact), Trade associations (27.9% high impact and 27.9% medium impact), cybersecurity professionals (14.3% high impact and 38.1% medium impact) and citizens (20% high impact and 70% medium impact).

Coherence with other legal instruments

The majority of trade associations, OESs & DSPs, and citizens rated the **coherence of the NIS Directive** as being medium and high. On the other hand, most of cybersecurity professionals and NCAs & CSIRTs thought the coherence was low and very low.

Vulnerability discovery and coordinated vulnerability disclosure

The respondents were asked to evaluate the level of effectiveness of national policies that are making vulnerability information available in a timelier manner. Just under a quarter of the

OPC respondents (24.8%) thought their level of effectiveness were medium, while 15.5% of the respondents rated the national disclosure policies as low or very low.

The OPC respondents were asked if their organisations have implemented a coordinated vulnerability disclosure policy. A significant proportion of the respondents did not respond or indicated this did not apply to them or their organisation (48%, 99 out of 206 respondents). 57 respondents went on to argue that national authorities such as CSIRTs could take proactive measures to discover vulnerabilities in ICT products and services provided by private companies.

Next steps

The Commission is now carrying out a deeper analysis of the replies received. The results, which are non-binding for the Commission, will feed into the Commission's proposals in the course of 2020.