Department for
Digital, Culture
Media & Sport

# Security of Network and Information Systems

Analysis of responses to public consultation

**January 2018**
**Department for Digital, Culture, Media and Sport**

## CONTENTS

## 1. Contact Details

This document is the post-consultation summary of the response to the consultation paper, *Security of Network and Information Systems Public Consultation of August 2017*. It will cover:

- a summary of the responses

Comments on the Government's analysis can be sent to:

NIS Directive Team
Department for Digital, Culture, Media & Sport
4th Floor
100 Parliament Street
London
SW1A 2BQ

Telephone: 020 7211 6000.
Email niscallforviews@culture.gov.uk

This report is also available at www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive. Alternative format versions of this publication can be requested from the above address.

Complaints or comments If you have any complaints or comments about the consultation process you should contact the NIS Directive Team at the above address.

*Freedom of Information*

Information provided in the course of this consultation, including personal information, may be published or disclosed in accordance with access to information regimes, primarily the Freedom of Information Act 2000 (FOIA) and the Data Protection Act 1998 (DPA).

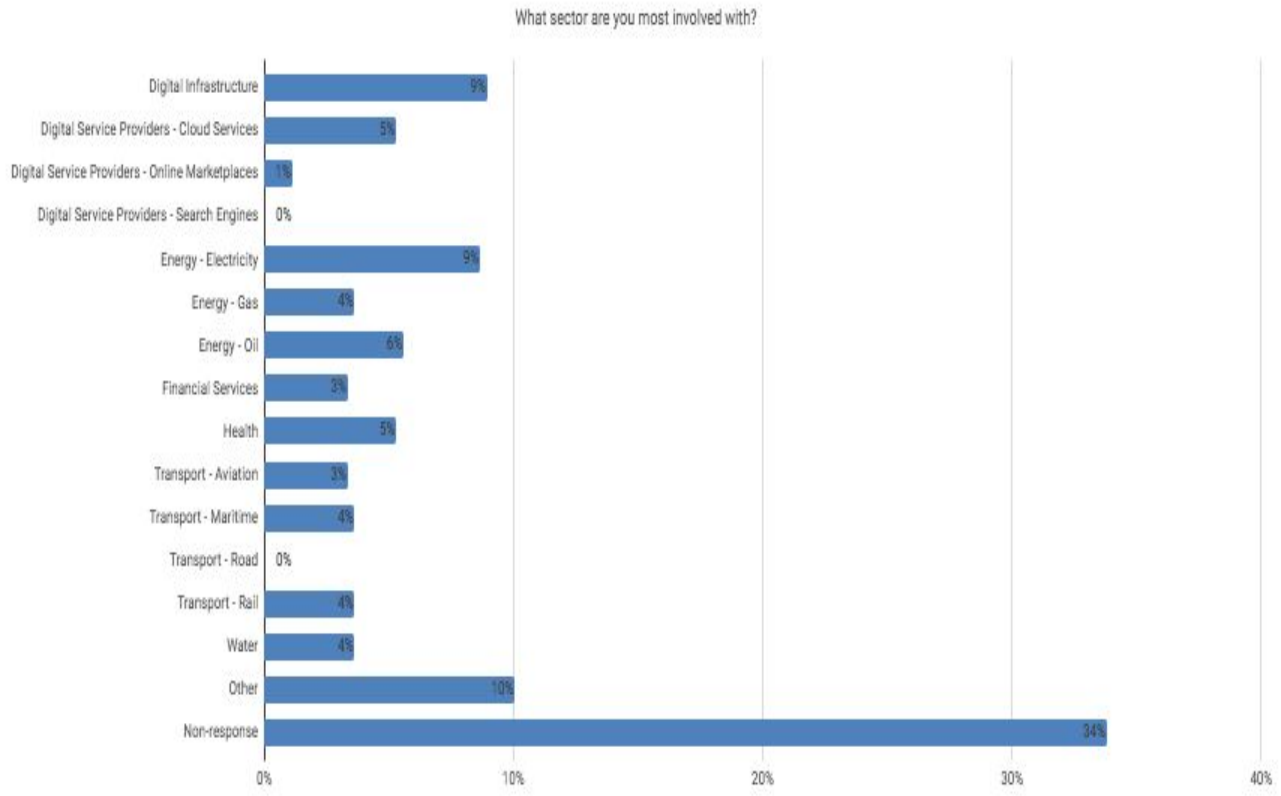
The Department for Digital, Culture, Media and Sport will process your personal data in accordance with the DPA and, in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties. This consultation follows the UK Government's consultation principles.

## 2. Consultation statistics

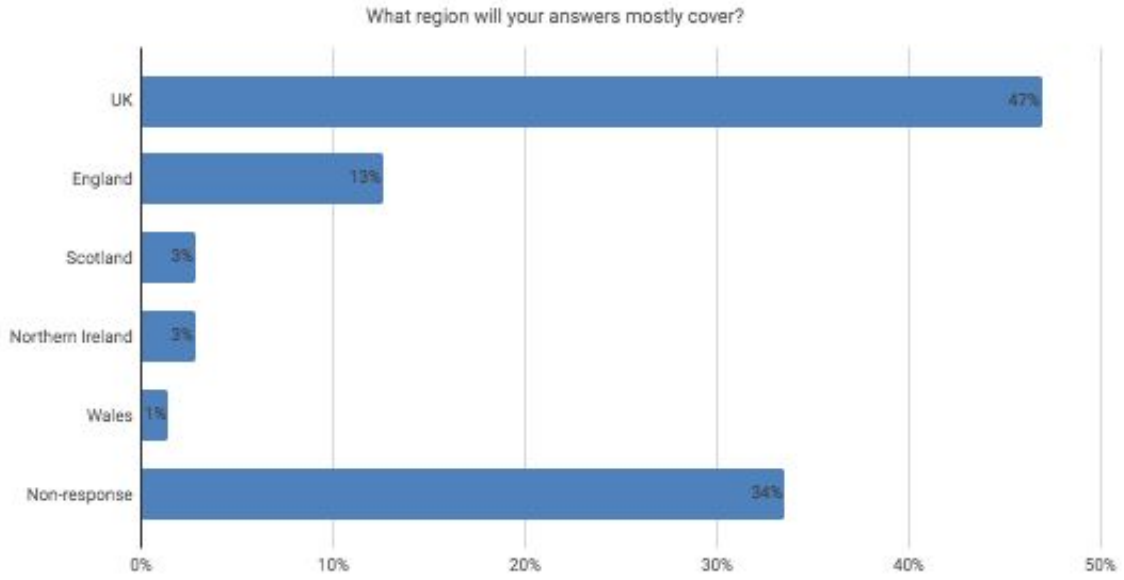
The Government received 358 substantive or partial responses to its consultation paper, *Security of Network and Information Systems Public Consultation* of August 2017. Of these responses, 294 were received via the online portal and 64 were written responses.

255 respondents replied on behalf of an organization and 103 replied as individuals.

Of those who indicated their primary sector, the majority of respondents were related to the Energy Sector (64), followed by 38 from the Transport Sector, 32 from Digital Infrastructure Sector, 23 were Digital Service Providers, 19 from the Health Sector, 13 from the Water Sector and 12 from the Financial Services Sector.




The majority of respondents who indicated the region their response covered said they cover the UK as a whole (168 respondents), with 45 indicating England, 10 indicating Scotland, 10 Wales, and 5 Northern Ireland.




## 3. Essential Services

Q1 Are the identification thresholds set at a level that captures the most important operators in your sector based on their potential to cause a significant disruptive effect if disrupted? YES/NO

Q2 If not, why not? What would you change and why?
Narrative response?

Questions 1 and 2

41% of respondents who submitted an answer to Q1 did not agree that the identification thresholds captured the most important operators, whilst 39% did and 19% did not know . Not all respondents subsequently provided comments to Q2, and some of those that did provide comments to Q2 did not state an answer to Q1. 85 responses to Q2 contained substantive comments, of which approximately 40% of these were from the energy sector (or were energy related).

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 62 | 13 | **75** | 39% |
| No | 45 | 34 | **79** | 41% |
| Don't Know | 36 | 1 | **37** | 19% |
| Non-response | 151 | 16 | **167** | |

Stakeholders provided mixed feedback on whether the thresholds were set at an adequate level,  with certain sectors considering the thresholds were too broad, and others considering the thresholds to be too narrow.

Many respondents noted that the thresholds/existing scope did not incorporate a number of additional sectors or service providers that they considered should be captured. Some of the examples of how respondents wanted the scope expanded included:

- Government
- Financial sector (banking, securities and investment).
- Audio Visual and Media
- Water Management (dams, storage, treatment and networks)
- Military and Defence industry
- Space and Research
- Production, storage, usage and transport of dangerous goods
- Emergency Services
- Food and Agriculture
- Pharmaceutical Industry
- Education
- Data Centres (t was noted that the DSP element seems to be very internet focused as the expense of other digital/comms elements of the sector)
- Operators providing services to immobile/vulnerable consumers

A number of recipients suggested an alternative approach to designation, such as creating a strategic business impact assessment, to allow businesses to determine themselves whether they are an essential service.

Some stakeholders were unclear about whether the thresholds applied to specific assets or to a business overall. Related to this was the comment that the Directive should apply even if a group of companies split themselves up into separate legal entities to avoid meeting the thresholds (eg, risk of gaming).

Questions were asked around whether regional impacts had been sufficiently considered, such as market share, geographic spread or availability of alternative facilities/suppliers. It was noted that an incident affecting a number of customers below the established thresholds would also likely be considered a ‘significant’ event. Several respondents also noted that the thresholds don’t actually identify the systems that will be in scope, and that clarifying this will be key.

Questions were raised around the proposed reserve power to designate, predominantly concerning how it was going to be used, what it applies to, and how much notice would be given.

## 4. National framework

Q3 Do you agree with the government's proposed approach of adopting a multiple competent authority model.

Q4 If not, why do you believe a single competent authority model represents a better option? Do you have an alternative outside of these two models?

Q5 Is the proposed competent authority for your sector a suitable choice?

Q6 If NO, who do you believe should be the competent authority for your sector and why?

Questions 3 and 4

70% of respondents who submitted an answer to Q3 supported the government's proposed approach of adopting a multiple competent authority, with 21% disagreeing and 9% undecided.

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 93 | 33 | 126 | 70% |
| No | 25 | 13 | 38 | 21% |
| Don't Know | 14 | 2 | 16 | 9% |
| Non-response | 162 | 16 | 178 | |

Of the total number of respondents who support the Government's approach, only a very few of those did so with caveats and proposed adjustments within the written responses. The majority of these related to ensuring consistency of approach and the need for coordination and cooperation between the Competent Authorities, including mandatory sharing of information and best practice. The need to coordinate in areas of shared jurisdiction was also mentioned.

Less than half of respondents provided a substantive answer to Q4. Of these the majority raised concerns about the multiple competent authority approach. Concerns ranged from consistency/clarity, coordination/response, funding and resources, to technical expertise. There were a moderate number of respondents who suggested a multiple competent authority model with caveats, and a small number who proposed an alternative model in

detail. There were very few respondents who noted potential conflict with other regulators and multiple competent authorities both nationally and internationally.

A number of respondents proposed an enhanced role for the NCSC with a small number suggesting the NCSC itself should be a single Competent Authority for the UK. This was on the basis that the NCSC had greater technical expertise and was already the focal point for cyber security in the UK. A general theme was the need for clarity in assigning roles and responsibilities, especially in maintaining an independent regulatory authority for enforcement and fines.

A number of respondents raised concerns about the proposals for Competent Authorities in the devolved administrations, primarily in Northern Ireland and Scotland.

Some recipients also highlighted a need for more clarity in the roles and responsibility of the Competent Authority and the NCSC. Particularly where the Competent Authority may retain some functions but delegate others to other regulators.

A number of recipients stressed the need for strong cooperation amongst Competent Authorities to ensure consistency in setting requirements and coordination during incident response. There were also concerns around the level of technical skills and expertise that the Competent Authority would have. Several responses referenced the need to strengthen the role of the NCSC as much as possible to provide guidance and support to Competent Authorities.

Some Operators of Essential Services were concerned about having more than one Competent Authority either nationally or internationally because their operation spans across sectors and/or countries. There was a suggestion that each Operators should agree a single authority that has oversight where they cross jurisdictions. The ICO raised a concern about incident notifications and commented that the requirement to notify NCSC under NIS would not satisfy the requirements to inform the ICO of data breaches under the GDPR.

A number of responses flagged concerns about conflicts of interest or introducing barriers to collaboration if the audit role is not separate from the role of setting principles, standards or providing technical expertise. There were also conflicts of interest raised with other regulatory or oversight responsibilities (e.g. DfT rail franchising). A number of energy sector respondents mentioned potential conflict with the emerging role of the HSE. Some concerns were also raised about the lack of an identified Competent Authority for the NI energy sector. Other concerns were around ensuring that the CAs are appropriately funded and resourced.

<u>Questions 5 and 6</u>

54% of respondents who submitted an answer to Q5 said their proposed competent authority was a suitable choice, whilst 46% (63) did not agree with the choice (no undecided option was available).

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 56 | 19 | 75 | 54% |
| No | 39 | 24 | 63 | 46% |
| Non-response | 199 | 21 | 220 | |

The majority of respondents who answered this question were broadly content with the proposed Competent Authority, but often with caveats or concerns regarding implementation. These were primarily focused on potential issues around overlap with other regulators or the ability of the Competent Authority to implement the Directive (largely based on a perceived lack of expertise).

Of those that did not agree with the proposed competent authority the following alternatives and explanations were given:

- A small number suggested the NCSC should be the Competent Authority. The majority of these also preferred a single national competent authority approach. The most common justification for suggesting the NCSC was to ensure the Competent Authority had the right skills and expertise. Many also felt this would enable consistent standards to be applied across sectors and avoid conflicts of interest.
- A similar level of respondents suggested an alternative sector regulator, which included suggestions of delegation from the Government Department to the regulator (such as BEIS delegating to OfGem or the Health and Safety Executive (HSE)) to separate compliance functions from standard setting, ensure better consistency with other regulatory regimes, and avoiding any conflicts of interest. However, some also noted that these concerns might be resolved by providing more clarity on the specific roles and responsibilities of the different organisations involved.
- A very small number did not specify any alternatives but raised the same concerns mentioned above with the current proposal (clarity of roles/responsibilities and how compliance will be conducted; cooperation between all entities with interest in cyber security).
- There were a few replies that suggested the ICO as a possible single competent authority.

Very few respondents offered an alternative model to that proposed in the consultation. One respondent proposed that the NCSC received all incident reporting before triaging for the sector Competent Authorities. Others saw an enhanced role for an independent body (especially for compliance) - either an existing regulator or the ICO.

## 5. Security requirements for operators of essential services

Q7 Do you believe these high level principles cover the right aspects of network and information systems security to ensure that risks will be appropriately managed?

Q8 If NO, can you clarify what aspects you believe are missing and recommend how we could address these?

Q9 Do you believe these principles would impose any additional costs on designated operators, or on the sectors in scope as a whole?

Q10 If YES, what do you consider would be the anticipated resource implication on designated operators, or on the industry as a whole of meeting these principles? Are you able to elaborate on the nature of these costs? Where possible please detail any specific financial costs you consider would likely result.

Q11 Do you have any plans to make additional security related investments as a result of this Directive? Where possible please indicate the size of investment (in £)?

Q12 If YES, please provide the amount and details of what investments would be required.

Questions 7 and 8

Over half of respondents who submitted an answer to Q7 believed the proposed high level principles covered the right aspects of network and information systems security, with almost a third disagreeing and only a few saying that they did not know.

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 68 | 27 | 95 | 58% |
| No | 33 | 17 | 50 | 31% |
| Don't know | 16 | 2 | 18 | 11% |
| Non-response | 177 | 16 | 193 | |

There were 106 respondents answering Q8 and clarifying the aspects they believed were missing. Of these, a small number responses focussed on the lack of detail within the principles and supporting explanation. Just under a quarter of respondents, a proportion of whom had responded positively to the principles themselves, raised concerns about how they would be applied in practice. These concerns were mainly in two areas. The first was the expectation that Operators of Essential Services would be held to account for the

application of the requirements throughout their supply chain, with the concern being the ability of companies to enforce the requirements on their 3rd party suppliers. The second was a concern about the extent to which the requirements, as a whole or in part would be made mandatory, or what would be considered an 'acceptable minimum' standard.

A small number of respondents requested that existing standards be used to assess compliance with NIS. The standards most frequently identified were ISO27001 and the US NIST Framework. Others included ISA/IEC62443, CAS(T), and the recently published Cyber Security Principles for the Water Industry. One respondent highlighted a perceived gap in the principles in relation to the link to GDPR.

There were a similarly small number of respondents, mainly from the energy sector, who focussed their concerns on applying the proposed principles to legacy systems in the Industrial Control Systems (ICS) environment.

A few respondents, from the rail, water and energy sectors, highlighted that the requirements focus on security rather than wider resilience or preventing disruption to supply.

A small number of respondents challenged the concept of NIS as a whole, or the proposed outcome based approach to regulation using principles and guidance. A similarly small number of respondents raised concerns with the wording of specific principles. The principles challenged in detail were 'B3 Data Security', 'B4 System Security', 'C1 Security Monitoring' and 'C2 Anomaly detection'.

Amongst the written responses, a moderate amount included narrative supportive of the proposed approach, including offers from companies to work with NCSC in the development of the proposed supporting guidance.

Questions 9 and 10

Almost three quarters of respondents who submitted an answer to Q9 believed these principles would impose additional costs with, 9% believing they would not and 20% saying that they did not know.

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 85 | 35 | 120 | 71% |
| No | 13 | 2 | 15 | 9% |
| Don't know | 18 | 15 | 33 | 20% |
| Non-response | 178 | 12 | 190 | |

Q10 asked respondents to elaborate further on the nature of costs corresponding to the high level security principles and what these costs might be. The primary response from a moderate number of respondents was around the cost of increasing staff resources, recruiting additional staff, improving training to provide additional readiness, and the cost of security software to meet requirements. A second point made by a few respondents respondents was around the need for additional information in order to be able to provide realistic costings - they noted that without this information it is challenging for organisations to be able to provide specifics. The third point, made by a small number of respondents was around the cost of installing additional infrastructure. In keeping with the previous point, respondents mentioned that further information was needed before specific costs could be given. The final point made by a small number respondents, was around the costs of compliance or Governance and this ranged from a single respondent mentioning the cost of certification to Cyber Essentials to establishing additional monitoring and controls to meet security requirements.

Questions 11 and 12

Almost half of respondents who submitted an answer to Q11 had plans to make additional security related investments as a result of this Directive, with 27% of these respondents saying they had no plans, and 31% saying that they did not know (or that it was too early to say).

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 44 | 19 | 63 | 42% |
| No | 32 | 8 | 40 | 27% |
| Don't know | 34 | 12 | 46 | 31% |
| Non-response | 184 | 25 | 209 | |

When asked for more detail on (Q12), the size of the investment (in £), about a third of respondents provided an answer. The majority responded with either a range of qualitative answers specifying areas of investment, or asking for additional information. Where organisations responded with a specific value it fell into one of four broad ranges. The first was from £0 - £50k, the second from £50k - £200k, the third £200k - £1M and the fourth was £1m or more (although this was often spread over a number of years).

In keeping with previous questions the majority of respondents felt that they did not have enough information to be able to provide the amount and details of any further security investments. The two themes that stood out for requiring additional resources were staffing, IT, and training and Governance and oversight. Some organisations said they had existing investment or plans outlined but no further information was given. Where figures were provided, this was only by a small number respondents and they were in the range of

£50,000 to over £1 million - again the breadth of the range suggesting costs of investments are difficult to estimate clearly.

## 6. Incident reporting for operators of essential services

Q13 Do you consider these incident reporting proposals to be reasonable to ensure that serious incidents affecting the network and information systems of essential services are reported?

Q14 If NO, why not? Can you suggest revised incident reporting proposals that ensure serious incidents are reported?

Q15 Do you consider that the proposed timeframe for providing incident reports place an undue burden on designated operators of essential services?

Q16 If YES, can you explain what these burdens and costs would be?

Questions 13 and 14

Half of respondents who submitted an answer to Q13 considered these incident reporting proposals to be reasonable, with just under half believing they were not, and very few remaining undecided. Although a majority of respondents supported the proposals, there were clear divisions between sectors to the Government's approach, with the majority of health, digital and water sectors respondents in favour of the proposals, whilst the energy sector strongly opposed.

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 57 | 23 | 80 | 50% |
| No | 42 | 22 | 64 | 40% |
| Don't know | 13 | 2 | 15 | 9% |
| Non-response | 182 | 17 | 199 | |

180 respondents suggested revised incident reporting proposals (Q14). The main objection was the potential of over-reporting or duplication of reporting, followed by the need for further clarification. There were suggestions that reporting should be aligned with existing cross-sector and sector specific reporting regulations e.g. GDPR or Drinking Water Inspectorate. An element of mistrust on information sharing was shown by a handful respondents who proposed that incident reporting should be anonymous. Reporting thresholds were thought to be unclear as well as definitions of what constituted a reportable incident. Respondents commented that the wording was ambiguous and it was not clear

what constituted a significant incident or what was in scope. The information required for incident reporting was also unclear, for instance format and update schedules but only by a very small number of respondents. Concern was expressed about the lack of clarity on incident reporting being used to attribute blame or liability for incidents, again only by a small number of respondents.

Concern was expressed over the undue burden that these incident proposals would place on organisations at a time when their focus would be on operational management and mitigating the incident. This impact would probably be greatest on smaller companies.

Questions 15 and 16

Over half of respondents who submitted an answer to Q15 considered that the proposed timeframe for providing incident reports would not place an undue burden on designated operators with, about third who believed they would and a small number who did not know.

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 29 | 12 | 41 | 28% |
| No | 63 | 23 | 86 | 59% |
| Don't Know | 17 | 1 | 18 | 12% |
| Non-response | 185 | 28 | 213 | |

When asked about the timeframe for providing incidents reports (Q16) some respondents felt that this placed an undue burden on designated operators of essential services. 78 respondents provided a substantive response.

The main point by just under half of respondents was that the timescale was not appropriate. This response covered a range of issues including noting that 72 hours was too short, a timeframe shouldn't be specified, and allowing organisations to report outside of the 72 hours when they can justify why. Almost a third of the respondents said that there would be a staffing burden as a result, including needing to employ extra staff as well as an increased burden on staff of completing the reporting process. The third point with only a small number of respondents was that the burden was unquantifiable at this stage, and that further information would be required. A fourth point made, again by only a small number of respondents, was around the burden of investigating the incident, including coordinating with third party response team, and the remediating action necessary. A single respondent said that their current systems won't register an incident so they would be unable to report it.

## 7. Digital service providers (DSP)

Q17 Are Digital Service Providers easily able to identify themselves using these criteria?

Q18 If NO, Why Not? Can you provide revised criteria that would identify providers more easily?

Q19 Would using these definitions create any unfair competitive advantage or disadvantage for Digital Service Providers within scope?

Q20 If you answered YES to the previous answer , please clarify nature of the advantage or disadvantage?

Definitions

Just over a third of respondents who submitted an answer to Q17 considered that Digital Service Providers could easily identify themselves using these criteria, with a fairly even split between those believing they were not, and those who did not know.

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 44 | 6 | 50 | 39% |
| No | 20 | 20 | 40 | 31% |
| Don't know | 38 | 0 | 38 | 30% |
| Non-response | 192 | 38 | 230 | 128.00 |

The two main themes respondents raised in response to Q18 were the need for broader parameters such as adding integration services, content providers, data centres and managed services, and the need for better definitions for Cloud and Software as a Service (SaaS). A few respondents objected in principle to including DSPs or objected to the business to business focus, and a similar few suggested avoiding SaaS completely.

Some respondents said that the definitions were too narrow and that all DSPs should be covered by the Directive as many businesses rely on the internet and digital services, whilst others thought the definitions were too generic. One respondent was concerned that the consumer market may not be able to provide the necessary level of scrutiny and due diligence.

*Online marketplaces*

There was a concern that large enterprises could circumvent the controls intended for Online Markets by tweaking their business model to become resellers rather than sales facilitators. One respondent wanted clarification as to whether classified platforms were included, as the current definition could be read as including them.

*Search engines*

One respondent raised  a concern that the the definition of search engines does not take into account search engines designed to discover vulnerabilities and potential breaches. Another said that as search engines could not search all websites using this definition would exclude any search engine.

*Cloud Services*

The majority of respondents focused on cloud services. There were concerns that the criteria was not clear enough and that the use of the term cloud itself was misleading. A number of respondent disagreed with the use of IaaS, PaaS and SaaS as descriptors, and questioned what would happen if a new type of Cloud service is produced as there were already emerging technologies and architectures that do not fit well into the IaaS, SaaS, PaaS taxonomy. One respondent recommended using ISO standards to define cloud computing.

Respondents raised concerns about whether specific aspects of cloud services were covered, such as reselling (reselling products rebranded as their own), hybrid cloud and private cloud, internal and external cloud, data centres and integration service providers.

A number of companies raised concerns over the inclusion of SaaS in the definition of cloud services, stating that virtually all online services have a SaaS element. SaaS could be interpreted to include finance, human resources and stock control and could create an artificial distinction and burden for cloud based solutions rather than on premises or outsourced.

A small number of respondents were concerned over smaller companies, who might offer bespoke and niche services for the management of operational assets, who are unlikely to recognise that they  would come under the category of cloud computing. There was also a concern over the scale regarding cloud services and the thresholds that will apply.

Finally a number of respondents were concerned at the proposal to focus on business to business (B2B) SaaS. B2B services are subject to contract, due diligence on both parties and only the customer is ultimately able to understand the role the services play in their operations. This approach goes against the normal principle that consumers are at a disadvantage and need additional regulatory protection whereas business users are required to be competent and diligent and protected by competition law.

Questions 19 and 20

Less than one fifth of respondents who submitted an answer to Q19 agreed that using these definitions would create any unfair competitive advantage or disadvantage for Digital Service Providers, with fewer believing they would not, than those stating that they did not know.

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 11 | 8 | 19 | 17% |
| No | 28 | 4 | 32 | 28% |
| Don't know | 63 | 0 | 63 | 55% |
| Non-response | 192 | 52 | 244 | |

Only a small number of respondents provided a substantive answer to how the definitions would cause a competitive advantage or disadvantage (Q20). The main theme raised, but only by very few respondents in total, was that respondents felt there would be a competitive advantage to big DSPs or those not applying to NIS. The second theme was from those who felt there would be a disadvantage to cloud, IaaS providers, and online vs offline companies. The third point was from those who felt there would be a disadvantage to non-NIS compliant DSPs. The final point by a single respondent was a question over how these definitions would be applied to the supply chain.

Some respondents thought that these requirements would disadvantage cloud service providers against traditional hosting or managed service providers, as the latter would not need to comply with the Directive. Another thought that it was not appropriate to treat cloud based applications differently in security terms compared to onsite premises or outsourced solutions.

Some respondents highlighted the competitive advantage this will give to larger DSPs, who would be more able to comply with the requirements of the Directive. Smaller organisations would maybe struggle to compete against the larger DSPs and Operators of Essential Services are likely to only contract with those DSPs who were NIS accredited to ensure that their overall services were compliant. There was a risk of potential abuse by large players in so far as that they can use economic strength to restrict, distort or eliminate competition as well as undermining the e-commerce security intent of the Directive. Stating that a DSP was NIS compliant, or even covered by NIS may for example give customers, such as Operators of an Essential Service, comfort that the DSP's services are compliant and that the DSP is aware of the NIS Directive. Whereby smaller organisations who do not need to be aware of the Directives or complaint may lose opportunities as they are not able to state that they are subject to NIS and not therefore demonstrate that they are fully compliant.

One respondent said that IaaS providers in particular would be disadvantaged as they do not necessarily see the data they are processing, or know the service they are hosting. Providers should not be held liable for what isn't known.

One respondent asked how the DSP supply chain would work, especially when there were multiple (sub)contracts. They gave an example of when an Operator of an Essential Service contracts with a supplier, who then subcontracts to another supplier, who then subcontracts to a third supplier. Would all three subcontracted suppliers be covered by the directive?

## Security requirements for DSPs

| |
|---|
| Q21 Are these principles reasonable?<br><br>Q22 If NO, Why not? Can you suggest revised principles that would enable important incidents to be reported?<br><br>Q23 What would be the impact on your business in applying these principles?<br><br>Q24 Do you have an alternative preferred approach? |

Almost two thirds of respondents who submitted an answer to Q21 agreed that the principles were reasonable, with about a tenth believing they would not, and a quarter stating that they did not know.

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 61 | 13 | 74 | 64% |
| No | 9 | 2 | 11 | 10% |
| Don't know | 29 | 1 | 30 | 26% |
| Non-response | 195 | 48 | 243 | |

*Security Principles*

Only a small number of respondents (21 in total) answered the question of how to revise the principles (Q22). Of these half respondents suggested amendments to the principles, with the majority saying they needed to be less ambiguous and the others saying they needed an additional principle. Other points raised by small numbers of respondents were the need for cultural, skills and leadership change, the need to revise the risk principles, the concern that these would disadvantage SMEs, and the need to maintain consistency with the GDPR.

Respondents highlighted a general concern that the principles were too ambiguous and subject to too much interpretation. Security controls needed to be in appropriate to the risk

appetite of your organisation. In general, these are reasonable. Mapping or alignment to a framework like the 10 steps would be beneficial, and another said that many of the organisations that will be required to adhere to the requirements under ENISA will not be able to comply.

Others said that a lot depends on how "measures in place are, where possible, compatible or comparable to internationally recognised cyber security standards" is interpreted. It was essential that cyber security standards that are suitable and designed for SMEs can be used, and noted that large organisations and government often underestimate how hard it is for SMEs to achieve standards designed for large companies.

A single respondent said that there needed to be an additional principle of transparency for clients/customers. There should ideally be an expectation that customers are notified about an incident in a timely manner. Another said that the scope of principle D "capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, services" should be reviewed as this may be the most onerous in terms of cost and resource to meet. Another highlighted the need to include good security leadership, adequate skills and capabilities, good threat intelligence and most importantly that Education and Awareness to reduce people related risk is key to future cyber risk control. Cultural change should be part of the Directive.

A couple of respondents highlighted the need for consistency with GDPR terminology or a statement that these security principles were in addition to any GDPR requirement.

*Costs of implementation*

57 respondents provided information of the impact of these principles (Q23). There were three main themes - the reassurance that NIS implementation will bring to customers; the specific measures DSPs will need to take, and the need to ensure consistency across Europe. Almost half of these respondents noted that more information was required or that costs were unclear. The secondary themes included a fifth who said there would be a financial impact and these values were from £10k - £200k in range. There were also about a fifth of respondents who objected in principle, said they were not a DSP, or who said the principles should be aligned to international standards.

A number of non-DSPs submitted responses to this question, highlighting the benefits and reassurance that applying the principles would bring. Amongst the comments made were that it would "*set reasonable expectations of the service delivery partners*", "*improve confidence that they had implemented suitable safeguards to keep the service functioning*", and "*provide assurance that our supply chain was more secure*". A single respondent said that it would prevent unsafe businesses undercutting responsible organisations. Another respondent said that it may require smaller businesses to pay for cyber security consultancy services and that procurement of such services must be assisted by clear standards for qualification of such consultants. A single respondent said that reliance by critical operators on DSPs, including telecoms providers should be taken into account when establishing what appropriate and reasonable plans are. There was a potential impact on procurement choices

when selecting digital services providers depending on their compliance levels with the directive.

A number of respondents highlighted particular areas that would be impacted:

- ICT teams.
- New hardware for monitoring / protection.
- review and publication of updated policies
- testing any new systems and infrastructure
- map our Governance, Policy and Procedures to the NIS Directive
- identification and remediation of systems and infrastructure that is not compliant with the directive
- resource and systems to prevent or minimise incidents

Other respondents were less specific, saying that they would pull elements managed from different parts of the business into an overall management system or would reorganise existing structures to fit the to framework developed within this directive. Some respondents said that there would be no major impact, and that their existing policies and structures covered these requirements already. A single respondent in the Health sector highlighted the difficulties they face in funding anything not seen as direct patient care. A single respondent said that only small adjustment in reporting processes and further consideration on how we gain effective assurance would be needed. One respondent stated that additional resource to improve the governance and reporting of cyber incidents, which would cost of around £50,000 - £60,000 a year.

A few respondents highlighted the importance of maintaining EU harmonization and mutual recognition, as divergence would have an impact on importers especially in a post Brexit environment. Another was concerned about matching EU requirements too closely, saying that DSPs should be provided a level of flexibility when putting in place their baseline security measures and that a direct obligation to include any of the measures and elements set out in the European Commission's Implementing Act would not respect the light touch approach of the Directive. Others highlighted the importance of using existing international standards.

*Alternative approaches*

30 respondents provided an alternative to the government's response (Q24). Quarter of these respondents suggested including other components such as pen testing, adding an additional sector, and including threat intelligence. A fifth of respondents suggested implementing the principles in a different manner. There were calls for greater clarity from a fifth of respondents as well as suggesting using international standards, also from a fifth of respondents as the principles of security requirements. The third and final point made was that respondents didn't know or didn't have an alternative approach with only a few respondents for each of these.

On specific amendments or alternatives, respondents suggested a number of options:

- An online portal to gather this information from each of our 3rd parties and hosting partners to building a picture where this is going to have the biggest impact.
- Implementing the Directive by phases
- Excluding resilience elements and focusing on cyber attacks only
- Including the financial sector
- Including the need for security leadership, adequate skills and capabilities, good threat intelligence and Education and Awareness.
- Including globally recognised standards
- Including SME focused standards
- Make compliance a Legal requirement and prosecute those that do not comply.
- Mandatory Penetration tests conducted by a third party.
- Mandatory ISO/CISO roles
- Mandatory compliance and auditing
- Making the Framework the same as that for Operators of Essential Services
- Ensuring existing cyber policies reflect these principles.

A couple of respondents raised concerns over the European Commission's draft Implementing Act, highlighting the need to ensure DSPs remain free to implement security baseline measures as they see fit and that the Uk follows the light touch approach.

Several respondents highlighted the difficulty in determining alternatives as the terms of the principles are are vague, and that further clarification was required of expectations, scoping and eventual compliance. Another said that the principles are too subjective and that a DSP could argue they adhere to the requirements and still fail to meet the expectations of the Government.

## Incident Reporting for DSPs

Q25 Would this incident reporting timeframe place an undue burden on your business or operations?

Q26 If YES, can you explain what these burdens and costs would be?

Q27 Do you wish to take part in the proposed targeted consultation exercise once the security and incident reporting thresholds have become clearer?

Q28 If YES, please provide an appropriate name, and email address for future correspondence.

About a fifth of respondents who submitted an answer to Q25 believed that this incident reporting timeframe place an undue burden on your business or operations, with half believing they would not, and a third stating that they did not know.

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 12 | 9 | 21 | 19% |
| No | 51 | 7 | 58 | 51% |
| Don't know | 32 | 2 | 34 | 30% |
| Non-response | 199 | 46 | 245 | |

*Costs and Burdens*

Respondents were asked about the incident reporting timeframe and whether this would place an undue burden on their organisation. The main point by a small number of respondents noted a burden would be identifying who owns the fault. The secondary point said the burden would be changes to the type of reporting required, changes to thresholds, and that it would inhibit information sharing. The third point made was that timescales needed to be modified with only a few responses saying they were too long and a couple saying they were too short. The final point from a few of the respondents was around burdens of changes to confidentiality .

The majority of respondents supported the proposed incident reporting timeframe. However, some did not. A single respondent noted the importance of promptness when notifying the competent authority about a serious incident, but said a specific timeframe is was too strict. In the event of a serious incident, the foremost priority for the affected entity should be stopping or containing the incident, and fixing the vulnerability or error that caused it. There was a risk that if containing the breach is left until after a notification is issued, the risk of harm arising from the breach would increase. A single respondent asked what happens if 72 hours is too little? Another respondent said that the timeframe for initial reporting was too long. A single respondent said that the implications for their business could be huge, especially when the supply chain is not theirs to control. There were concerns that there need to be enough time to identify, mitigate, or remedy the incident, understand the root cause and whether it lays with the DSP or a contractor.

A small number of respondents were concerned over the thresholds for incident reporting. A single recommended focusing on availability and refraining from referencing integrity and confidentiality. A single respondent raised concerns over the European Commission's proposed thresholds, stating that they were too low thresholds and risked the possibility of over-reporting by DSPs. On the use of number of users as a parameter, they raised concerns that many DSPs would find it difficult to calculate the total number of users affected by a cyber incident. The geographic threshold was also difficult for DSPs to monitor. Another single respondent recommend that DCMS work with the NCSC and the designated competent authorities to define this reporting process and provide the tangible examples of the types of incidents / events that are expected to be reported.

The interaction of DSPs and Operators of Essential Services was raised by several respondents. One respondent stated that Operators of Essential Services would need to understand accountabilities for reporting of incidents given that the DSPs could be reporting incidents impacting on many OES organisations. They asked how would this be controlled and communicated given all the different sectors potentially involved needs to be considered? Another asked if there was a requirement for them to inform their customers, especially if customer is an Operator of Essential Services?

A single respondent raised concerns over the practical burden of reporting to multiple places. Depending on the circumstances, a DSP may have to report the incident to three different organizations: the Assistant Authority (CSIRT), the Supervisory Authority (Competent Authority), and in some cases also to the Information Commissioner's Office. This creates a situation where a company affected by a serious hack will have to spend a lot of precious time and resources to proceed with up to three separate notifications in a very short time-frame all at a time when the company will rightly be focussed on remedying the incident itself.

Finally a small number of respondents raised concerns of the confidentiality of any information that they shared. A single respondent stressed the need for confidentiality of both voluntarily and mandatorily reported security incidents, which may contain company sensitive information, stating that the comfort of confidentiality will increase the willingness of companies to report security incidents which will improve the overall cybersecurity and visibility on volumes for the authorities.

*Further targeted consultation*

A large number of respondents indicated a desire to be involved in a further targeted consultation on the DSP aspects. The statistics for this have not been analysed as they are not directly related to the proposals. EU Member States have yet to agree the final version of the European Commission's Implementing Act for DSPs, without which it is difficult to set the specific parameters. When this Implementing Act has been agreed, DCMS will initiate a further targeted consultation.

A number of these who requested to be part of this targeted consultation did not respond to any of the DSP questions, and it appears there may have been some misunderstanding that the targeted consultation applied more widely than just DSPs. It is DCMS's intention to further consult only on the DSP aspects. DCMS therefore intends to contact only those respondents who are either DSPs or whose substantive response included comments on the DSP aspects.

## 8. Penalty regime

| |
|---|
| Q29 Do you consider the proposed penalty regime to be proportionate to the risk of disruptions to operators of essential services? |

Q30 Do you believe that the proposed penalty regime will achieve the outcome of ensuring operators take action to ensure they have the resources, skills, systems and processes in place to ensure the security of their network and information systems?

Q31 If you answered NO to either of these two questions, please explain how the penalty regime could be amended to address your concerns.

Just over a third of respondents who submitted an answer to Q29 considered the proposed penalty regime to be proportionate to the risk, with over half of these believing they were not, and a tenth of these stating that they did not know.

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 45 | 9 | 54 | 37% |
| No | 43 | 35 | 78 | 53% |
| Don't know | 12 | 2 | 14 | 10% |
| Non-response | 194 | 18 | 212 | |

Almost half of respondents who submitted an answer to Q30 considered that the proposed penalty regime would achieve the outcome of ensuring operators take action. However, a similar, but slightly fewer, number believed that the regime would not achieve that outcome. A tenth of respondents stated that they did not know.

| Answer | Online Response | Written Response | Total Responses | % Who Answered |
|---|---|---|---|---|
| Yes | 47 | 12 | 59 | 42% |
| No | 36 | 25 | 61 | 44% |
| Don't Know | 17 | 2 | 19 | 14% |
| Non-response | 194 | 25 | 219 | |

*How should the regime be amended?*

The main point by a majority of respondents on proportionality (Q31) noted that the penalty regime needed changing with answers ranging from saying it was too high, saying the split of penalties was wrong, and saying the regime was not proportionate. The two secondary points were the need to address behavioural / market impacts and the need to deconflict

with other regimes and both of these answers were similarly close in number to the main response.

The proposed regime was considered to be too severe when compared to other EU Member States, where penalties ranged from €20,000 to €5m. However many respondents also noted that it was difficult to assess the proportionality of the penalty regime without further detail around the intended application and needed this to be clarified. Respondents suggested that the potential consequences of a regime which was too severe included:

- the exit of operators from UK markets due to economic disadvantage of operating here;
- reduction in the financial viability of their business models or risk to their financial stability resulting from any fines.

A key concern raised was clarifying the approach to dealing with cases of 'double jeopardy' where incidents could result in penalties under the NIS Directive, GDPR and other regulatory frameworks such as the Control of Major Accident Hazards (COMAH) Regulations. A few comments highlighted the regulatory tensions between e.g. NIS Directive and financial stability (potentially also diversity of suppliers etc).

Many considered that the proposed penalties were too severe or not necessary given that operators of essential services would bear costs to the business in terms of loss of revenue, brand damage, breaches of contract or other regulatory damage and felt these business incentives were sufficient to drive investment.

Some observed the proposed alignment in penalty structure between the GDPR and the NIS Directive and felt this was not appropriate given the differing objectives and application of the two frameworks.

A number of respondents felt that the penalties for DSPs should be lower in the light of lower potential impact of a DSP service outage.

Several companies operating in multiple EU Member States called for a consistent approach and close working with other Member States on designation, security requirements and incident reporting.

In some cases respondents felt that the penalties would threaten the financial stability of companies (through fines or in competitive low-margin sectors) and in some cases this was in direct tension with regulatory objectives on financial resilience.

A small number of respondents felt that the split of the penalty bands was not appropriate. Many respondents felt that it was disproportionate that penalties were proposed to apply to a percentage of global turnover and felt that penalties should be linked to UK turnover or UK turnover in relation to essential service provision only.

Respondents' views were finely balanced in support of whether the proposed penalty regime will achieve the outcome of ensuring operators take action to ensure they have the resources, skills, systems and processes in place to ensure the security of their network and information systems. A moderate number of respondents said the regime incentivises wrong behaviour, with a similar number saying it could lead to risk of market exit, and a similar amount disagreeing with what the penalties apply to. On the deconfliction with other regimes, a moderate number of respondents noted the need to deconflict with GDPR and others noted the need to deconflict with other regulatory regimes. The third point suggested a need to address how the regime is enforced. The final point with only a very modest response rate suggested the penalty regime was not relevant.

Many considered that penalties, or the threat of penalties to be applied in the most egregious cases, were necessary but not in themselves sufficient to drive change. However some were concerned that a heavy-handed approach could fundamentally damage valuable existing voluntary arrangements and collaboration between operators and Government. A number were concerned that their designation as an operator of essential service in itself would make them a more high-profile target, or that focus on security requirements could divert investment from incident response capability.

A small number of respondents queried the potential for an appeals process. Others similarly raised issues around working between Competent Authorities within the UK, across England, Northern Ireland, Scotland and Wales.

A very small number of respondents considered the penalty regime was too low and that further criminal sanctions should be considered.