Department for Digital, Culture, Media & Sport

Security of Network and Information Systems

Government response to targeted consultation on Digital Service Providers

August 2018

Department for Digital, Culture, Media and Sport

CONTENTS

1. Contact details

This document is the Government's response to the public consultation, *Security of Network and Information Systems targeted consultation on Digital Service Providers of April 2018*.

Comments on the Government's response 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. Executive summary

On March 2018, the Government published a targeted consultation on how the Security of Network and Information Systems Directive (known as the NIS Directive) will apply to Digital Service Providers (DSPs) in the UK. This consultation covered three main topics -

- Identification of DSPs
- Security measures
- Further guidance

The Government received 12 responses to its consultation. The majority of responses indicated there was broad support for the Government's overall approach towards digital service providers, but there continued to be uncertainty over exactly who was in scope - particularly in relation to cloud service providers - and that greater clarification was needed on the subject of cost recovery.

The Network and Information Systems Regulations 2018 (NIS Regulations) are now in effect. The Government therefore proposes to use the outcome of this consultation to assist the Information Commissioner's Office (ICO) in clarifying its guidance to digital service providers. The key areas the Government will look to clarify are:

- How DSPs can more easily identify whether they are within scope of the NIS Regulations;
- How cloud services in particular are defined; and
- How the ICO's cost recovery process will operate.

Background on the NIS Directive

The NIS Directive was adopted by the European Parliament on 6 July 2016. Member States have until 9 May 2018 to transpose the Directive into domestic legislation. The NIS Directive provides legal measures to boost the overall level of network and information system security in the EU by:

- Ensuring that Member States have in place a national framework to support and promote the security of network and information systems, consisting of a National Cyber Security Strategy, a Computer Security Incident Response Team (CSIRT), a Single Point of Contact (SPOC), and a national NIS competent authority (or authorities);

- Setting up a Cooperation Group, to support and facilitate strategic cooperation and the exchange of information among Member States. Member States will also need to participate in a CSIRT Network to promote swift and effective operational cooperation on specific network and information system security incidents and as well as the sharing of information about risks;

- Ensuring the framework for the security of network and information systems is applied effectively across sectors which are vital for our economy and society and which rely heavily on information networks, including the energy, transport, water, healthcare and

digital infrastructure sectors. Businesses in these sectors that are identified by Member States as “operators of essential services” will have to take appropriate and proportionate security measures to manage risks to their network and information systems. Operators of essential services will also be required to notify serious incidents to the relevant authority. Key DSPs (search engines, cloud computing services and online marketplaces) will also have to comply with the security and incident notification requirements established under the Directive.

On 23 June 2016, the EU referendum took place and the people of the United Kingdom voted to leave the European Union. Until exit negotiations are concluded, the UK remains a full member of the European Union and all the rights and obligations of EU membership remain in force. During this period the Government will continue to negotiate, implement and apply EU legislation. The outcome of the negotiations on the future UK-EU partnership will determine what arrangements apply in relation to EU legislation once the United Kingdom has left the EU. It is the UK Government’s intention that on exit from the European Union these policy provisions will continue to apply in the UK.

3. Consultation statistics

The Government received 12 responses to its consultation paper, *Security of Network and Information Systems targeted consultation on Digital Service Providers* of April 2018. Of these, 6 were received via the online portal and 6 were written responses (of which one written response was a supplement to their online response).

9 respondents replied on behalf of an organization and 3 replied as individuals.

Answer	Written	Online	Total	%
On behalf of an organisation	5	4	9	75%
As an individual	1	2	3	25%
Total	6	6	12	100%

Of those responders that indicated the sector that they were most involved with, five indicated DSPs as a whole, two indicated cloud services, and one indicated online marketplaces.

Answer	Responses	%
Digital Service Providers	5	63%
Digital Service Providers - Search Engines	0	0%
Digital Service Providers - Online Marketplaces	1	13%
Digital Service Providers - Cloud Services	2	25%
Total	8	100%

4. Identification of digital service providers

Q1 Are you readily able to identify yourself from the descriptions provided?

Q2 If No, please provide alternative descriptions that would improve the definitions.

Questions 1 and 2

55% of respondents who submitted an answer to Q1 stated that they could identify themselves from the descriptions provided, with 45% saying that they could not.

Answer	Written	Online	Total	%
Yes	0	6	6	55%
No	5	0	5	45%
Total	5	6	11	100%

The main concern regarding the definition of digital services providers related to the definition of cloud service provider, which five respondents commented on. Two responses questioned the UK's proposal to limit cloud services to public cloud services, stating that this departed from the NIS Directive approach, with one response saying that hybrid, private and community cloud should be included. One response questioned the definition of software as as service, stating that the definition was too broad and could include almost any online application. Another asked how elastic and scalable was defined.

One response focused on the definition for online marketplaces, raising concerns that a website offering differing services might be included as a whole, or whether a site where the payment service is provided via a third party is included. Another response requested further clarification on which marketplaces were covered by the legislation - is it covered by number of customers or the size of those customers?

Government Response

The Network and Information Systems Regulations 2018, which implement the NIS Directive into UK law, reflect carefully the language of the NIS Directive and the legal definition of a digital service provider is deliberately the same. However, interpreting this legal definition in a manner that is both compatible with the Directive and clear to individual DSPs continues to be a major challenge. As stated in the Government's response to the original public consultation on the UK's proposals for transposing the NIS Directive, the Government's intention has always been to try to make it clear who was in scope and who was without, and to limit the scope of those who have to comply with the Directive to those companies whose loss of service could have the greatest impact on the UK economy either directly or through impact on other companies.

The Government continues to believe that interpreting the definition of DSPs to include all online activity, or all activity that could potentially be classed as 'software as a service' is not

consistent with the NIS Directive. Cloud services are limited to those that are scalable and elastic - by which we mean computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand (scaleable) and computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload (elastic).

For online marketplaces, the Government is clear that the service has to be a genuine marketplace for goods or services and not an online retailer. Where a provider offers both retail services and online marketplace services, the online marketplaces services are covered by the NIS Directive. In relation to payment for those services, if a purchaser purchases a product from an online marketplace, and payment for that product takes places through services provided by that online marketplace (whether third party or not) then they are within scope of the NIS Regulations. If the online marketplace transfers the purchases to the original product seller's website, and the purchase and transaction take place there, then they are not within scope of the NIS Regulations. In relation to size, the primary requirement is that the DSP must be larger than a small or micro-sized business (i.e. have 50 or more staff and an annual turnover of €10m a year). The size of its marketplace, or number of customers is not considered in any assessment of a DSP. If only part of a DSP's services are potentially within scope of the NIS Regulations, then the Government advises that the DSP contact the ICO (nis@ico.org.uk) to seek clarification on how the Regulations will apply.

Where a prospective DSP is unclear about whether or not they are in scope of the NIS Regulations, they are strongly advised to contact the ICO (nis@ico.org.uk) for clarification.

5. Security measures

Q3 Are the security requirements set out above understandable to you?

Q4 If no, please provide examples of specific areas so that further guidance on the security requirements can provide clarification?

Questions 3 and 4

73% of respondents who submitted an answer to Q3 stated that the security requirements were understandable, with 27% saying that they were not.

Answer	Written	Online	Total	%
Yes	3	5	8	73%
No	2	1	3	27%
Total	5	6	11	100%

Although the majority of respondents were clear about the security requirements of NIS, a number raised some specific questions. One respondent highlighted concerns on how to balance the requirements set out in the proposed Regulations and those set out in the Commission's implementing regulations. The same respondent also asked how risk will be defined, and what information should be reported to the ICO. One respondent emphasised the importance of emphasising that "*DSPs remain free to implement security baseline measures as they see fit, provided that they provided adequate and sufficient security*", and that common international standards such as ISO27001 and the NIST Framework be used as sufficient to demonstrate compliance. They also requested further guidance on how DSPs could effectively calculate many of the incident reporting parameters. Another respondent requested that the NIS security guidelines for DSPs be more fully aligned with those of the General Data Protection Regulation (GDPR), whilst one respondent requested specific testable standards like the Payment Card Industry Data Security Standard (PCI/DSS).

Government Response

It is important that whatever security and incident reporting measures that the UK Government puts in place for DSPs, that they are consistent with the Commission's implementing Regulation and are compatible with those being put in place across Europe. This is important because many DSPs operate across Europe and differences would be an unwelcome burden on business. As such, the NIS Regulations 2018 specifically require DSPs to meet the requirements set out in the Commission's implementing regulations.

The requirements on DSPs are set out in Regulation 12 of the Network and Information Systems Regulations 2018. This section includes the security and incident reporting requirements for DSPs.

The ICO is responsible for publishing further guidance on how digital service providers can meet the security requirements set out in the NIS Regulations. The Government has recommended to the ICO that they advise digital service providers to follow the technical guidance published by the European Network and Information Systems Agency.

In relation to the GDPR, the National Cyber Security Centre and the ICO have already published their GDPR security outcomes to provide guidance to organisations considering GDPR in a cyber context. These requirements are fully compatible with those set out by ENISA for digital service providers.

6. Further guidance

Q5 Are there any areas of implementation of the NIS Directive that remain unclear, which the ICO in its capacity as Competent Authority can make clear in its guidance?

The main theme from all the response to this question was for the ICO to produce clear and comprehensive guidance for digital service providers on how they can meet the requirements of the NIS Regulations. In particular, respondents asked that the ICO provide specific guidance on:

- How the ICO will determine whether a NIS incident merits CSIRT attention.
- The scope of the non-disclosure power for the ICO (in relation to making issues public).
- How the ICO will define Software as a Service.
- The size of organisations to which the rules apply.
- How the ICO will handle or mitigate incidents that fall under NIS and the GDPR.
- Details on how the ICO intends to recover costs and the potential amount of fees
- How the penalty and appeal regime will work.
- Whether the NCSC could produce guidance on security measures for DSPs.

Government Response

Regulation 12 of the NIS Regulations 2018 sets out the requirements on DSPs and the scope of the ICO's remit as competent authority. Many of the answers to the queries raised in this consultation are set out in the Regulations. For example, Regulation 12(8) requires that the ICO to inform the CSIRT after receipt of every incident notification, 12(12) and 12(13) set out the non-disclosure powers of the ICO, and Regulation 1(3)(e) provides the definition of who is a relevant digital service provider.

The ICO is committed to provide comprehensive guidance on all aspects of its role as Competent Authority for digital service providers, and has already published its initial advice. The Government will continue to work with the ICO to support its NIS work and the ICO will provide updated guidance, including on the issues set out above, as soon as is feasible.