Department for Digital, Culture, Media & Sport

March 2018

Security of Network and Information Systems Targeted consultation on Digital Service Providers

In the Government's response to last August's security of Network and Information Systems (NIS) Directive public consultation, DCMS committed to carry out a targeted consultation on how NIS will apply to Digital Service Providers (DSPs) in the UK, once the European Commission's Implementing Act for Digital Service Providers was approved by Member States.

Subsequent to the Government's response, the Implementing Act was published in the Official Journal of the European Union on 30 January 2018 and can be found on the EUR-LEX website. It will come into force on 10 May 2018.

This paper is the Government's targeted consultation and is intended to seek views on how the Government intends to implement the NIS Directive as it applies to DSPs.

PLEASE NOTE:

- **This consultation is limited to how the UK proposes to implement and carry out the requirements of the Implementing Act, as neither the UK nor any other Member State has flexibility to amend the Implementing Act now that it has been agreed.**
- **References to the UK legislation relate to draft legislation. The final text may differ from that set out in this document. This consultation is not seeking comments on the draft legislation.**

How to respond

We welcome your views. To help us analyse the responses please use the online system wherever possible. Visit the Department's online tool to submit your response. Hard copy responses can be sent to:

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

Or emailed to niscallforviews@culture.gov.uk

The closing date for responses is 29 April 2018.

When providing your response, please also provide contact details - we may seek further information or clarification of your views.

Copies of responses, in full or in summary, may be published after the consultation closing date on the Department's website.

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 digital service providers (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.

Implementation of the NIS Directive as it applies to DSPs

Overall approach

The Government's approach is based around ensuring consistency across Europe, so that UK DSPs can have a consistent approach in regard to security measures across the UK and the rest of Europe. Both the Government and the Competent Authority (the Information Commissioner's Office) will approach implementation of the NIS Directive in a reasonable and proportionate fashion.

Identification of DSPs

As set out in the Government's Response, the UK will define DSPs in the same way as set out in the Directive:

- "**digital service**" means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council which is of the following type:
  (a) online marketplace;
  (b) online search engine; or
  (c) cloud computing service;

- "**digital service provider**" means any legal person that provides a digital service;

- "**online marketplace**" means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;

- "**online search engine**" means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input and returns links in which information related to the requested content can be found;

- **"cloud computing service"** means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

The Information Commissioner's Office (the ICO), as the Competent Authority for DSPs, will be responsible for regulating Digital Service Providers in the UK in the context of the NIS Directive. In order to assist DSPs in recognising when they are in scope of this Directive the ICO will produce guidance, which will be based on the Government's proposed clarifications which were set out in the Government's response:

"*Online marketplaces*

- An online marketplace should be defined as a platform that acts as an intermediary between buyers and sellers, facilitating the sale of goods or services, i.e. a service that enables consumers and traders to conclude online sales or service contracts with traders, and it represents the final destination for the conclusion of those contracts.

- Sites that redirect users to other services to make the final contract (e.g. price comparison sites), or that only connect buyers and sellers to trade with each other (e.g. classified advert sites), or that only sell directly to consumers on behalf of themselves (e.g. online retailers), are not in scope.

Online search engines

- 'online search engine' means a digital service that allows users to perform searches of the 'public parts of the worldwide web' in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.

- Where a site offers search engine facilities as outlined above, but those facilities are powered by another search engine, then the underlying search engine is required to meet the requirements of the NIS Directive. Internal organisational search engines, that do not facilitate external searches of the internet are not in scope.

Cloud computing services

- 'cloud computing service' means any digital service that enables access to a scalable and elastic pool of shareable physical or virtual resources.

- The Government considers that this primarily (but not exclusively) includes Digital Service Providers that provide public cloud services of the following nature:

    - "'Infrastructure as a Service' (IaaS) - the delivery of virtualised computing resource as a service across a network connection, specifically hardware – or computing infrastructure - delivered as a service;
    - 'Platform as a Service' (PaaS) - services that provide developers with environments on which they can build applications that are delivered over the internet, often through a web browser; and
    - 'Software as a Service' (SaaS), provided the resources available to the customer through that software are changeable in an elastic and scalable way. The Government considers that this would likely exclude most current online gaming, entertainment or VOIP services, as the resources available to the user are not scalable, but may include services such as email or online storage providers, where the resources are scalable." (pages 14-15 of the Government response to consultation)

Registration

The ICO will, after 10 May 2018, establish a system in order for UK DSPs to register themselves with the ICO. We are considering making registration mandatory. This

registration system is necessary in order for the ICO to know who is required to meet the requirements of the Directive and who they need to regulate.

Security Measures

Firstly it is important to note that DSPs are not required to meet the security requirements that were set out in the Government Consultation and Response, which only apply to Operators of Essential Services. The NIS Regulation will set out the security requirements for DSPs in accordance with the requirements in the Commission's Implementing Act.

The Implementing Act sets out the security requirements for DSPs as follows:

Article 2
Security elements

1. Security of systems and facilities referred to in point (a) of Article 16(1) of Directive (EU) 2016/1148 means the security of network and information systems and of their physical environment and shall include the following elements:

(a) the systematic management of network and information systems, which means a mapping of information systems and the establishment of a set of appropriate policies on managing information security, including risk analysis, human resources, security of operations, security architecture, secure data and system life cycle management and where applicable, encryption and its management;

(b) physical and environmental security, which means the availability of a set of measures to protect the security of digital service providers' network and information systems from damage using an all-hazards risk-based approach, addressing for instance system failure, human error, malicious action or natural phenomena;

(c) the security of supplies, which means the establishment and maintenance of appropriate policies in order to ensure the accessibility and where applicable the traceability of critical supplies used in the provision of the services;

(d) the access controls to network and information systems, which means the availability of a set of measures to ensure that the physical and logical access to network and information systems, including administrative security of network and information systems, is authorised and restricted based on business and security requirements.

2. With regard to incident handling referred to in point (b) of Article 16(1) of Directive (EU) 2016/1148, the measures taken by the digital service provider shall include:

(a) detection processes and procedures maintained and tested to ensure timely and adequate awareness of anomalous events;

(b) processes and policies on reporting incidents and identifying weaknesses and vulnerabilities in their information systems;

(c) a response in accordance with established procedures and reporting the results of the measure taken;

(d) an assessment of the incident's severity, documenting knowledge from incident analysis and collection of relevant information which may serve as evidence and support a continuous improvement process.

3. Business continuity management referred to in point (c) of Article 16(1) of Directive (EU) 2016/1148 means the capability of an organisation to maintain or as appropriate restore the delivery of services at acceptable predefined levels following a disruptive incident and shall include:

(a) the establishment and the use of contingency plans based on a business impact analysis for ensuring the continuity of the services provided by digital service providers which shall be assessed and tested on a regular basis for example, through exercises;

(b) disaster recovery capabilities which shall be assessed and tested on a regular basis for example, through exercises.

4. The monitoring, auditing and testing referred to in point (d) of Article 16(1) of Directive (EU) 2016/1148 shall include the establishment and maintenance of policies on:

(a) the conducting of a planned sequence of observations or measurements to assess whether network and information systems are operating as intended;

(b) inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, and efficiency and effectiveness targets are being met;

(c) a process intended to reveal flaws in the security mechanisms of a network and information system that protect data and maintain functionality as intended. Such process shall include technical processes and personnel involved in the operation flow.

5. International standards referred to in point (e) of Article 16(1) of Directive (EU) 2016/1148 mean standards that are adopted by an international standardisation body as referred to in point (a) of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council. Pursuant to Article 19 of Directive (EU) 2016/1148, European or internationally accepted standards and specifications relevant to the security of network and information systems, including existing national standards, may also be used.

6. Digital service providers shall ensure that they have adequate documentation available to enable the competent authority to verify compliance with the security elements set out in paragraphs 1, 2, 3, 4 and 5.

The security measures set out by the Commission are intended to be outcome focused. They do not specify how DSPs must implement them. The ICO, as the Competent Authority, will publish further guidance to ensure that DSPs understand their obligations under the Directive.

When producing this Guidance, the ICO will take into account the Technical Guidelines for the implementation of minimum security measures for Digital Service Providers published by the European Network and Information Systems Agency (ENISA) in 2017. This will ensure that there is a consistent approach across Europe.

The UK, in its Regulations to transpose the Directive into UK law, will not repeat these requirements, but will direct DSPs directly to this Implementing Act as follows:

(1) The measures taken by a RDSP [relevant Digital Service Providers] under paragraph (1) must—

(a) ensure a level of security of network and information systems appropriate to the risk posed;

(b) prevent and minimise the impact of security incidents affecting their network and information systems with the aim of ensuring the continuity of those services; and

(c) take into account the following elements—

(i) the security of systems and facilities;

(ii) incident handling;

(iii) business continuity management;

(iv) monitoring auditing and testing;

(v) compliance with international standards; and

(vi) the security elements mentioned in Article 2 of Commission Implementing Regulation (EU) 2018/151. [emphasis added]

Incident Reporting

Under the draft Regulations which transpose the Directive into UK law, a RDSP (relevant Digital Service Provider) must notify the ICO about any security incident which has a substantial impact on the provision of any of the following digital services: (a) online marketplace; (b) online search engine; or (c) cloud computing service. In order to determine whether the impact of a security incident is substantial an RDSP must have regard to a set of criteria set out in Article 3 and 4 of the Commission's Implementing Act. Additionally the draft Regulations provide that an RDSP must also have regard to the following:

(a) (in so far as the RDSP is able to assess), the number of users affected by the incident, and in particular, any users relying on the digital service for the provision of their services;
(b) the duration of the incident;
(c) the geographical area affected by the incident;

(d) the extent of the disruption to the service provision;
(e) the extent of the impact on economic and societal activities.

Article 3

Parameters to be taken into account to determine whether the impact of an incident is substantial

1. With regard to the number of users affected by an incident, in particular users relying on the service for the provision of their own services referred to in point (a) of Article 16(4) of Directive (EU) 2016/1148, the digital service provider shall be in a position to estimate either of the following:

(a) the number of affected natural and legal persons with whom a contract for the provision of the service has been concluded; or

(b) the number of affected users having used the service based in particular on previous traffic data.

2. The duration of an incident referred to in point (b) of Article 16(4) means the time period from the disruption of the proper provision of the service in terms of availability, authenticity, integrity or confidentiality until the time of recovery.

3. As far as the geographical spread with regard to the area affected by the incident referred to in point (c) of Article 16(4) of Directive (EU) 2016/1148 is concerned, the digital service provider shall be in a position to identify whether the incident affects the provision of its services in specific Member States.

4. The extent of disruption of the functioning of the service referred to in point (d) of Article 16(4) of Directive (EU) 2016/1148 shall be measured as regards one or more of the following characteristics impaired by an incident: the availability, authenticity, integrity or confidentiality of data or related services.

5. With regard to the extent of the impact on economic and societal activities referred to in point (e) of Article 16(4) of Directive (EU) 2016/1148, the digital service provider shall be able to conclude, based on indications such as the nature of his contractual relations with the customer or, where appropriate, the potential number of affected users, whether the incident has caused significant material or non-material losses for the users such as in relation to health, safety or damage to property.

6. For the purpose of paragraph 1, 2, 3, 4 and 5, the digital service providers shall not be required to collect additional information to which they do not have access.

Article 4
Substantial impact of an incident

1. An incident shall be considered as having a substantial impact where at least one of the following situations has taken place:

(a) the service provided by a digital service provider was unavailable for more than 5 000 000 user-hours whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes;

(b) the incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100 000 users in the Union;

(c) the incident has created a risk to public safety, public security or of loss of life;

(d) the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000 000.

The ICO may publish additional guidance for DSPs on the Commission's implementing act, however it should be noted that the impact parameters set out by the Commission are specific and the UK is bound by them.

The UK, in its regulations to transpose the Directive into UK law, will not repeat these requirements, but will direct DSPs directly to this Implementing Act as follows:

(1) A RDSP must notify the Information Commissioner ("the Commissioner") about any security incident having a substantial impact on the provision of any of the digital services mentioned in paragraph (1)(a) to (c).

(2) The notification under paragraph (3) must—

(a) be made as soon as possible and in any event no later than 72 hours after the service provider is aware that a security incident has occurred; and

(b) contain sufficient information to enable the Commissioner to determine the significance of any cross-border impact.

(3) In order to determine whether the impact of a security incident is substantial the RDSP must have regard to the following matters—

(a) (in so far as the RDSP is able to assess), the number of users affected by the incident, and in particular, any users relying on the digital service for the provision of their services;

(b) the duration of the incident;

(c) the geographical area affected by the incident;

(d) the extent of the disruption to the service provision;

(e) the extent of the impact on economic and societal activities; and

(f) **Articles 3 and 4 of Commission Implementing Regulation (EU) 2018/151.** [emphasis added]

DSPs who service an Operator of Essential Services

Where a DSP provides a service to an Operator of Essential Service, if they have an incident that impacts on the service of that Operator of Essential Service, it is the responsibility of the operator to inform the competent authority of the incident. This does not absolve the DSP of their responsibility to inform the ICO if they would otherwise be required to do so. The UK regulations will state:

> (1) If an operator of essential services relies on a RDSP for the provision of an essential service which is critical for [economic and societal functions], that operator must notify the relevant competent authority in relation to that operator about any significant impact to the provision of that essential service caused by a security incident as soon as the incident occurs.

If a DSP is an Operator of an Essential Service

If a DSP also provides a service that is classified as an 'Essential Service', and thus is an Operator of Essential Services under the NIS Directive, they will be obliged to meet the requirements of both a DSP and an Operator of Essential Services under the NIS Directive for the service that they provide.

Where they provide both DSP services and an Essential Service they should engage with the relevant Competent Authorities (for the essential service sector and for Digital Services) and reach an agreement as to which one they should report to if they would otherwise be required to notify to both. In such cases the Government will encourage Competent Authorities to talk to each other and agree a systems to minimise incident reporting. The OES/DSP will, however, have to meet the security and incident reporting requirements applicable to both Essential Services and DSPs.

Costs

The ICO, along with other Competent Authorities will have the power to recover the costs of regulating the NIS Directive. The UK's legislation will state that:

> **Fees payable by operators of essential services or relevant digital service providers**
> **1.** — A fee is payable by an operator of essential services or a RDSP to an enforcement authority, to recover the reasonable costs incurred by, or on behalf of that authority in carrying out the requirements set out in these Regulations.
> (1) The fee mentioned in paragraph (1) must be paid to the enforcement authority within 30 days after receipt of the invoice sent by the authority.
> (2) The invoice must state the work done and the costs incurred by or on behalf of the enforcement authority, including the time period to which the invoice relates.
> (3) A fee payable under this regulation is recoverable as a civil debt.
> (4) In this regulation "enforcement authority means—
> (a) the relevant competent authority in relation to an operator of essential services; or

(b) the Information Commissioner for RDSPs.

In this context, it is expected that the ICO, in line with common practice in other regulations such as the GDPR, will levy an annual fee on DSPs, in addition to recovering direct costs involved in any regulatory investigations. The amount of this fee has not yet been determined and will be published by the ICO in due course.

Questions for Digital Service Providers

1. Are you readily able to identify yourself from the descriptions provided?
   YES/NO

2. If No, please provide alternative descriptions that would improve the definitions.
   Narrative answer

3. Are the security requirements set out above understandable to you?
   YES/NO

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

5. 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?
   Narrative answer