Ofcom
making communications work for everyone

Ofcom's interim guidance for Operators of Essential Services in the digital infrastructure subsector under the Network and Information Systems Regulations 2018

Implementing the NIS Directive

GUIDANCE

Publication Date: 08 May 2018

About this document

This document provides Ofcom's interim guidance in relation to the so-called digital infrastructure subsector for which Ofcom has been designated as the competent authority for the United Kingdom under regulation 3(1) of the Network and Information Systems Regulations 2018 (S.I. 2018/506) (the "**NIS Regulations**"). This interim guidance is mainly directed to so-called operators of essential services (the "**OES**") providing essential services in relation to the digital infrastructure subsector.

In brief summary, this interim guidance:

- gives a high-level introduction to the NIS Regulations;
- sets our initial views on the immediate steps we expect the OES in the digital infrastructure subsector to take, as a minimum, to meet their obligations under the NIS Regulations;
- provides information about which types of operators on which duties have been imposed under the NIS Regulations;
- sets out the process and thresholds for reporting relevant security incidents that such operators must initially follow; and
- introduces our intended initial enforcement approach.

You will find at the end of this document links to the relevant Government statement providing background information on the NIS Regulations, and to guidance published by the UK's National Cyber Security Centre ("**NCSC**") intended to help companies comply with their obligations.

Contents

Section

Annex

1. Introduction

Role and Status

1.1 Guidance has the benefit of contributing to effective regulation by improving transparency and understanding. In particular, this interim guidance is aimed at encouraging compliance by explaining the OES' security duties and their duties to notify network and information systems incidents to Ofcom, thereby ensuring that they properly understand their obligations and enabling potential customers to identify any concerns.

1.2 One of Ofcom's regulatory principles is that Ofcom will regulate in a transparent manner[1]. Guidance can serve as a useful means to achieving this principle and to increasing understanding of Ofcom's policy objectives and approach to regulation. Furthermore, Ofcom must prepare and publish guidance in relation to the digital infrastructure subsector under regulation 3(3)(a) of the NIS Regulations.

1.3 The NIS Regulations were made on 19 April 2018. They come into force on 10th May 2018, including Ofcom's obligation to publish guidance. Ofcom has therefore had little time and opportunity to finalise any detailed guidance for the purposes of the NIS Regulations. As we are the newly appointed regulator for the digital infrastructure subsector under the NIS Regulations, we also expect that our initial guidance will need to evolve as we gain a better understanding of the sector, including in working with the OES, in continuing to discuss security requirements with the NCSC, the Department of Digital, Culture, Media & Sport ("DCMS") and other regulators, and in giving further consideration to the recent DCMS' guidance to Competent Authorities.

1.4 Accordingly, we are publishing this interim guidance for now to give enough information to the OES in the digital infrastructure subsector to ensure that initial practical and other arrangements are put in place, and that they take certain immediate steps, as a minimum, to meet their obligations under the NIS Regulations. We expect to review this interim guidance in due course and update it as necessary, including having regard to any feedback that we receive from the OES themselves. We will also consider adjusting the reporting process and thresholds in this interim guidance, if this proves necessary to ensure they work effectively. We encourage anyone with queries or feedback about the content of this interim guidance to contact us at nis@ofcom.org.uk.

1.5 Meanwhile, Ofcom would normally expect to follow this interim guidance should it investigate any breaches of the duties discussed. If Ofcom decides to depart from this interim guidance, we will set out our reasons for doing so. Any guidance we give now and, in the future, may also be subject to revision from time to time.

1.6 That said, whether or not (and, if so, how) a particular matter is regulated will usually turn on the specific facts in each case. Therefore, the OES should seek their own independent

[1] https://www.ofcom.org.uk/about-ofcom/what-is-ofcom

advice on specific matters, taking into account the facts in question to answer specific questions on their duties imposed under the NIS Regulations. Ofcom cannot, as a matter of law, fetter its discretion as to any future decision. Accordingly, although this interim guidance sets out the approach Ofcom would normally expect to take, this guidance does not have binding legal effect, and each case will be considered on its own merits.

The national framework under the NIS Regulations / the NIS Directive

1.7 The NIS Regulations implement Directive 2016/1148/EU concerning measures for a high common level of security of network and information systems across the European Union, i.e. the Network Information Services Directive (or simply the "**NIS Directive**")[2].

1.8 The UK currently remains a full member of the European Union and all of the rights and obligations of EU membership remain in force, including under the NIS Directive. The outcome of ongoing negotiations on the future UK-EU partnership will determine what arrangements apply in relation to EU legislation once the UK has left the EU. However, it is the UK Government's stated intention that on exit from the EU the policy provisions of the NIS Directive will continue to apply in the UK.

1.9 The NIS Directive aims to raise levels of the overall security and resilience of network and information systems across the EU.

1.10 The NIS Directive essentially requires that Member States implement a national framework to support and promote the security of network and information systems and the essential role those systems play in the national infrastructure of the UK. This framework for the UK includes under the NIS Regulations the establishment of:

- a National Cyber Security Strategy by the Government (regulation 2);
- a Computer Security Incident Response Team ("**CSIRT**") (regulation 5 designates GCHQ);
- a Single Point of Contact ("**SPOC**") (regulation 4 designates GCHQ); and
- designated competent authorities (i.e. regulators) for the respective subsectors in relation to which the OES provide essential services (regulation 3), the relevant broader sectors of which are Energy; Transport; Health; Drinking Water Supply and Distribution; and Digital Infrastructure.

1.11 The NIS Regulations contains threshold requirements for companies in each of the subsectors falling within those broader sectors. Entities which provide essential services that rely on network and information systems, and meet those thresholds are "deemed to be designated" as the OES and, as such, are therefore immediately subject to relevant duties in the NIS Regulations. Designated regulators also have powers to designate other entities not meeting those thresholds, provided that certain conditions are met.

1.12 As part of this national framework, the NIS Regulations particularly impose security duties (regulation 10) and duties to notify network and information systems incidents to their designated regulators within 72 hours of becoming aware of the incident (regulation 11).

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

1.13 DCMS published its consultation about the implementation of the NIS Directive in August 2017[3], and its response to the consultation [4]in January 2018. These documents contain more background information on the NIS Directive and the Government's approach to the UK's implementation.

The NCSC role in the NIS Directive

1.14 The NCSC is part of GCHQ and, as such, is providing technical support and guidance to other government departments, devolved administrations, designated regulators and the OES. It has, in particular, the following three roles under the national framework discussed above:

- **SPOC** – as already noted above, GCHQ is designated as the SPOC and, as such, the NCSC acts as the contact point for engagement with EU partners on issues relating to the NIS Directive, coordinating requests for action or information and submitting annual incident statistics.
- **CSIRT** – as already noted above, GCHQ is designated as the CSIRT and, as such, the NCSC discharges associated obligations under the NIS Regulations. For example, the NIS Regulations impose a duty on the OES to notify their designated regulators of certain security incidents with a significant impact. Where incidents are identified or suspected of having a cyber security aspect, the OES should also contact NCSC, in its role as the national CSIRT, for advice and support on these aspects.
- **Technical Authority on Cyber Security** – the NCSC will support the OES and designated regulators with cyber security advice and guidance and act as a source of technical expertise. The NIS Guidance Collection[5] brings together advice published by the NCSC that is relevant to the OES considering compliance with their duties under the NIS Regulations. In summary, it sets out:
  - 4 top-level security objectives;
  - A set of sector-agnostic Security Principles which support the delivery of these objectives. Each principle describes security outcomes to be achieved.
  - A Cyber Assessment Framework ("**CAF**") incorporating indicators of good practice.
  - However, the NCSC will not have a regulatory role as such under the NIS Regulations, which remit falls on each designated regulator.

[3] https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf

[5] https://www.ncsc.gov.uk/guidance/nis-guidance-collection

2. Ofcom as designated regulator for the digital infrastructure subsector

2.1 Ofcom is specified in column 3 of the table in Schedule 1 to the NIS Regulations as the "competent authority" for the "digital infrastructure subsector" and for the territorial jurisdiction of the United Kingdom. As such, Ofcom is a regulator designated under regulation 3(1) of the NIS Regulations. As regards that territorial jurisdiction, it should also be noted that regulation 1(6) of the NIS Regulations states that they apply to the UK (including its internal waters) and the territorial sea adjacent to the UK.

2.2 The notion of the "digital infrastructure subsector" has not been defined as such. However, the types of services falling within that subsector is discussed below.

2.3 In relation to that subsector, Ofcom must do the following things (regulation 3(3)):

- review the application of the NIS Regulations;
- prepare and publish guidance in such form and manner as Ofcom considers appropriate; such guidance may be reviewed at any time and any revised guidance must be published as soon as reasonably practicable;
- keep a list of all the OES who are designated, or deemed to be designated, under regulation 8, including an indication of the importance of each operator in relation to the subsector in relation to which it provides an essential service;
- keep a list of all the revocations made under regulation 9;
- send a copy of each of those lists mentioned to the SPOC to enable it to prepare the report mentioned in regulation 4(3);
- consult and co-operate with the Information Commissioner when addressing incidents that result in breaches of personal data; and

2.4 in order to fulfil the requirements of the NIS Regulations, consult and co-operate with:

- relevant law-enforcement authorities;
- competent authorities in other Member States;
- other competent authorities in the UK;
- the SPOC; and
- the CSIRT.

3. Ofcom's general duties

3.1 It should also be noted that section 3 of the Communications Act 2003 imposes general duties on Ofcom in carrying out our functions, including under the NIS Regulations. That section 3(1) provides that it is Ofcom's principal duty to further the interests of citizens in relation to communications matters (i.e. matters in relation to which Ofcom has functions), and to further the interests of consumers in relevant markets, where appropriate by promoting competition.

3.2 In performing those general duties, Ofcom must have regard, in all cases, to:

i) the principles under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed; and any other principles appearing to Ofcom to represent the best regulatory practice.

3.3 OFCOM must also have regard, in performing those duties, to such factors listed in section 3(4) as appear to Ofcom to be relevant in the circumstances, such as the desirability of promoting and facilitating the development and use of effective forms of self-regulation.

4. OES designated for the digital infrastructure subsector

The OES "deemed to be designated" for the digital infrastructure subsector

4.1 Regulation 8(1) of the NIS Regulations "deems" certain entities as designated OES for the digital infrastructure subsector, without the need for Ofcom to take any decision to designate them as such. That regulation provides that:

4.2 "8.—(1) If a person provides an essential service of a kind referred to in paragraphs 1 to 9 of Schedule 2 and that service—

a) relies on network and information systems; and

b) satisfies a threshold requirement described for that kind of essential service, that person is deemed to be designated as an OES for the subsector that is specified with respect to that essential service in that Schedule."

4.3 In that regard, the following definitions in regulation 1 should be noted that:

"**essential service**" means a service which is essential for the maintenance of critical societal or economic activities; and

"**network and information system**" ("NIS") means—(a) an electronic communications network within the meaning of section 32(1) of the Communications Act 2003; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under paragraph (a) or (b) for the purposes of their operation, use, protection and maintenance;

4.4 Section 32(1) of the Communications Act 2003 defines an "electronic communications network" as follows:

4.5 "(1) In this Act "electronic communications network" means—

a) a transmission system for the conveyance, by the use of electrical, magnetic or electro-magnetic energy, of signals of any description; and

b) such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals—

i) apparatus comprised in the system;

ii) apparatus used for the switching or routing of the signals; . . .

iii) software and stored data; and

iv) (except for the purposes of sections 125 to 127) other resources, including network elements which are not active."

4.6 For the purpose of understanding that definition, the following definitions in the Communications Act 2003 should also be noted:

- a "**transmission system**" includes a reference to a transmission system consisting of no more than a transmitter used for the conveyance of signals (section 32(6));
- the "**conveyance of signals**" include references to the transmission or routing of signals or of parts of signals and to the broadcasting of signals for general reception (section 32(8));
- "**apparatus**" includes any equipment, machinery or device and any wire or cable and the casing or coating for any wire or cable (section 405(1));

4.7 the cases in which software and stored data are to be taken as being used for a particular purpose include cases in which they (a) have been installed or stored in order to be used for that purpose; and (b) are available to be so used (section 32(9)); and

4.8 a "**signal**" includes

a) anything comprising speech, music, sounds, visual images or communications or data of any description; and

b) signals serving for the impartation of anything between persons, between a person and a thing or between things, or for the actuation or control of apparatus.

4.9 In light of the above-mentioned regulation 8(1), it is necessary to consider the threshold requirements laid down in paragraph 10[6] of Schedule 2 to the NIS Regulations. That paragraph 10 essentially deems three categories of specified kinds of essential services as designated OES for the digital infrastructure subsector, each of which we discuss below.

First category of deemed OES: Top Level Domain Name Registries

4.10 The first category of specified kinds of essential services deemed as designated OES for the digital infrastructure subsector is the following kind of essential service that relies on network and information systems:

> "*For the essential service of Top Level Domain ("TLD") Name Registries the threshold requirement in the United Kingdom is TLD Registries who service an* ***average of 2 billion or more queries in 24 hours for domains registered within the Internet Corporation for Assigned Names and Numbers***." (paragraph 10(2) of Schedule 2 to the NIS Regulations) (emphasis added)

4.11 "**TLD Name Registry**" is a reference to "top-level domain name registry" which means an entity which administers and operates the registration of internet domain names under a specific top-level domain (paragraph 10(5)(d) of Schedule 2 to the NIS Regulations).

---

[6] W*hile we note that regulation 8(1) only refers to an essential service of a kind referred to in "paragraphs 1 to 9 of Schedule 2", we understand that this regulation contains a typographical error and should, in fact, have referred to paragraphs 1 to 10 of Schedule 2. (The same typographical error appears in regulation 8(3)(a).) We assume that DCMS will seek to correct this error in the NIS Regulations as soon as possible and we proceed in this interim guidance on the assumption that this error will be so formally corrected.*

Second category of deemed OES: Domain Name Service Providers

4.12 The second category of specified kinds of essential services deemed as designated OES for the digital infrastructure subsector is the following kind of essential service that relies on network and information systems:

4.13 "*For the essential service of Domain Name System ("DNS") Service providers the threshold requirement in the United Kingdom is—*

a) DNS service providers with an establishment in the United Kingdom who provide DNS resolvers offered for use by publicly accessible services, ***which service an average of 2,000,000 or more requesting DNS clients based in the United Kingdom in 24 hours****; or*

b) DNS service providers with an establishment in the United Kingdom who provide authoritative hosting of domain names, offered for use by publicly accessible services, ***servicing 250,000 or more different active domain names****." (paragraph 10(3) of Schedule 2 to the NIS Regulations) (emphasis added)*

4.14 In that regard, it should be noted that:

- "**DNS**" is a reference to "domain name system" which means a hierarchical distributed naming system in a network which refers queries for domain names (paragraph 10(5)(a) of Schedule 2 to the NIS Regulations);

- **"DNS service provider"** is a reference to "domain name system service provider" which means an entity which provides DNS services on the internet (paragraph 10(5)(b) of Schedule 2 to the NIS Regulations);

- **"DNS resolvers"** is not defined in the Regulations. However, Ofcom understands this to refer to recursive resolvers - client facing servers in the DNS hierarchy which manage the process of resolving client DNS requests to IP addresses.

Third category of deemed OES: Internet Exchange Point Operators

4.15 The third (and final) category of specified kinds of essential services deemed as designated OES for the digital infrastructure subsector is the following kind of essential service that relies on network and information systems:

> *"For the essential service of Internet Exchange Point (IXP) Operators the threshold requirement in the United Kingdom is* ***IXP Operators who have 50% or more annual market share amongst IXP Operators in the United Kingdom****, in terms of interconnected autonomous systems,* ***or who offer interconnectivity to 50% or more of Global Internet routes****." (paragraph 10(4) of Schedule 2 to the NIS Regulations) (emphasis added)*

4.16 **"IXP"** is a reference to "internet exchange point" which means a network facility which (i) enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; (ii) provides

interconnection only for autonomous systems; and (iii) does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor does it alter or otherwise interfere with such traffic (paragraph 10(5)(c) of Schedule 2 to the NIS Regulations).

Your statutory duty to notify Ofcom by 10th August 2018 if you are deemed to be designated

4.17 Regulation 8(2) imposes the following statutory duty:

- "(2) A person who falls within [regulation 8(1)] must notify the designated competent authority of that fact before the notification date."

4.18 Regulation 8(11) defines the "notification date" as:

- 10th August 2018, in the case of a person who falls within regulation 8(1) on the date the NIS Regulations come into force (i.e. 10th May 2018);
  in any other case, the date three months after the date on which the person falls within that paragraph

4.19 ****IMPORTANT NOTE:** You therefore have a duty to notify Ofcom **at the latest on 9th August 2018** if you fell within any of the three above-mentioned three categories of deemed OES on 10th May 2018. If you would fall within any of the three above-mentioned three categories of deemed OES at any time after 10th May 2018, you have a duty to notify Ofcom at the latest three months after the date on which you fell within such a category. Any such notifications should be done by emailing nis@ofcom.org.uk, with "NIS designation notification" in the subject line and should include the category or categories under which you fall and contact details to which we can direct follow up enquiries.

Ofcom's powers to designate additional entities as OES

4.20 Even if an entity does not meet the threshold requirements set out in the NIS Regulations (i.e. it falls outside any of the three above-mentioned three categories of deemed OES), Ofcom has the power under regulation 8(3) to designate it as an OES for the digital infrastructure subsector, but only if the following conditions are met:

- it provides an essential service of a kind specified in paragraph 10 of Schedule 2 to the NIS Regulations for the digital infrastructure subsector;
- its provision of that essential service relies on network and information systems; and
- Ofcom concludes that an incident affecting the provision of that essential service by that entity is likely to have significant disruptive effects on the provision of the essential service.

4.21 In order to arrive at that conclusion concerning the likelihood of significant disruptive effects, we must under regulation 8(4) have regard to the following factors:

- the number of users relying on the service provided;
- the degree of dependency of the other relevant sectors on the service provided;

- the likely impact of incidents on the essential service provided, in terms of its degree and duration, on economic and societal activities or public safety;
- the market share of the essential service provided;
- the geographical area that may be affected if an incident impacts on the service provided;
- the importance of the provision of the service by that company for maintaining a sufficient level of that service, taking into account the availability of alternative means of essential service provision;
- the likely consequences for national security if an incident impacts on the service provided; and
- any other factor Ofcom considers appropriate to have regard to.

4.22 Before Ofcom designates any entity as an OES, we may under regulation 8(6):

- request information from that entity by serving an information notice under regulation 15(4) of the NIS Regulations requiring it to provide us with information needed to assess whether to designate it; and
- invite the entity to submit any written representations about our proposed decision to designate it as an OES.

4.23 Although the Regulations do not require us to undertake the two steps above before designating an entity, we would normally expect to do so, unless exceptional circumstances applied.

4.24 Additionally, before Ofcom designates any entity as an OES, we must under regulation 8(7) consult with the relevant authorities in another Member State, if that entity already provides an essential service in that Member State.

4.25 The way in which Ofcom designate an OES is by notice in writing served on the person who is to be designated in accordance with regulation 24 of the NIS Regulations and provide our reasons for the designation in the notice.

Ofcom's maintenance of lists of designations, including their review

4.26 As already noted above, Ofcom must keep a list of all the OES who are designated, or deemed to be designated, under regulation 8, including an indication of the importance of each operator in relation to the subsector in relation to which it provides an essential service.

4.27 Ofcom is required by regulation 8(9) to review that list at regular intervals, the first of which must take place before 9th May 2020, and subsequent reviews taking place biennially.

Ofcom's powers to revoke OES designations

4.28 Ofcom has the power under regulation 9(1) to revoke a deemed OES designation falling within the three above-mentioned three categories, if we conclude that an incident affecting the provision of that essential service is not likely to have significant disruptive

effects on the provision of the essential service. In order to arrive at that conclusion concerning the likelihood of significant disruptive effects, we must under regulation 9(4) have regard to the above-mentioned factors in regulation 8(4).

4.29 We can also revoke under regulation 9(2) any OES designations we have ourselves made under regulation 8(3), if its conditions for designation are no longer met.

4.30 We further have the power under regulation 9(5) to revoke a deemed OES designation, or any OES designations we have ourselves made under regulation 8(3), if we have received a request from another Member State to do so and we are in agreement that the designation of that entity should be revoked.

4.31 Before revoking any designations, we must under regulation 9(3):

- serve a notice in writing of proposed revocation on the designated entity;
- provide reasons for our proposed decision;
- invite the entity to submit any written representations about our proposed decision within such time period as we may specify; and
- consider any representations submitted by the entity before a final decision is taken to revoke the designation.

4.32 The way in which Ofcom revoke designations is by notice in writing served on the person who has been designated in accordance with regulation 24 of the NIS Regulations.

OES security duties

4.33 Regulation 10 of the NIS Regulations imposes on designated OES the following security duties:

i) "(1) An OES must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies.

ii) (2) An OES must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.

iii) (3) The measures taken under paragraph (1) must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed.

iv) (4) Operators of essential services must have regard to any relevant guidance issued by the relevant competent authority when carrying out their duties imposed by paragraphs (1) and (2)."

4.34 In that regard, we note that, as required by regulation 10(3), the measures to be taken under regulation 10(1) by designated OES for the digital infrastructure subsector must ensure a level of security appropriate to the risk presented "having regard to the state of

the art" and therefore we would ourselves have regard to the state of the art of such measures in any compliance assessment by such OES.

4.35 We are not, however, in a position to give any further guidance in this interim guidance at this stage for reasons explained above [under Role and Status]. However, we would, as noted above, refer OES to guidance published by NCSC[7] in relation to the NIS Regulations.

OES duties concerning security incident reporting

Notifiable NIS incidents

4.36 Regulation 11(1) of the NIS Regulations imposes on designated OES in the digital infrastructure subsector a duty to report to Ofcom any incident which has a significant impact on the continuity of the essential service which it provides (i.e. **"a NIS incident"**). Such reporting should be done "*without undue delay and in any event no later than 72 hours after the operator is aware that a NIS incident has occurred*" and "*in such form and manner as* [Ofcom] *determines*" (regulation 11(3)(b)).

4.37 In determining the significance of the impact of an incident, an OES must under regulation 11(2) have regard to the following factors:

- the number of users affected by the disruption of the essential service;
- the duration of the incident;
- the geographical area affected by the NIS incident; and
- any relevant guidance issued by Ofcom (regulation 11(12))(see below for Ofcom's guidance).

4.38 We are required under regulation 11(5) to assess whether any further action is required in respect of a reported NIS incident and to share the NIS incident information with the NCSC, in their role as the UK CSIRT, as soon as reasonably practicable.

4.39 We are further required under regulation 11(9) to provide a report to the SPOC identifying the number and nature of NIS incidents notified to us. Our first report must be submitted on or before 1st July 2018 and subsequent reports must be submitted annually.

Ofcom's process requirements for security incident reporting

4.40 Regulation 11(3)(a) lists the essential requirements to be included by OES in a report to Ofcom, namely the report must provide the following information:

- the operator's name and the essential services it provides;
- the time the NIS incident occurred;
- the duration of the NIS incident;
- information concerning the nature and impact of the NIS incident;
- information concerning any, or any likely, cross-border impact of the NIS incident; and

[7] https://www.ncsc.gov.uk/guidance/nis-guidance-collection

- any other information that may be helpful to Ofcom.

4.41 However, that information is limited to information which may reasonably be expected to be within the knowledge of that OES (regulation 11(4)).

4.42 As noted above, security incident reporting must be done in such form and manner as Ofcom determines and OES must also have regard to any relevant guidance issued by Ofcom when OES carry out their duties imposed by regulation 11(1) to (4).

4.43 ****IMPORTANT NOTE:** In that regard, it should be noted that NIS incident reports should be submitted to incident@ofcom.org.uk. If OESs require a more secure method of communication, for example an e-mail address with enhanced security, this can be arranged. We will consider in due course whether there is benefit in introducing a secure reporting portal.

4.44 Such reports should be submitted on the form linked to below, including as much information as is reasonably available at the time of reporting. Noting that the duty imposed on OES to report "without undue delay", and in any event within 72 hours of the OES becoming aware of the NIS incident, it is possible that complete information will not be available at the time of the report. In such cases, additional information should be provided as it becomes available, but meanwhile the OES in question should not withhold reporting until more complete information is available.

4.45 ****IMPORTANT NOTE:** OES should also provide Ofcom with a general NIS incident contact point for enquiries about incidents which we become aware of, but which have not yet been reported.

4.46 OES should note that, like the other designated regulators for the NIS Regulations, Ofcom's role does not include incident response. OES should therefore not view NIS incident reporting to us as any substitute for reporting to other agencies which provide specific support. As such, OES, and indeed any other companies in the sector suffering from a cyber security incident with which they require assistance or technical support, should contact the NCSC through the usual channels, as soon as possible. Similarly, if the incident may be criminal in nature, the appropriate law enforcement agency should be contacted.

4.47 **NIS incident report form:**
https://www.ofcom.org.uk/__data/assets/rtf_file/0025/113749/Network-and-Information-Systems-incident-report-form.rtf

Ofcom's guidance on the significance of the impact of an incident (i.e. reporting thresholds)

4.48 ****IMPORTANT NOTE:** As noted above, one of the factors that OES must have regard to in determining the significance of the impact of an incident is any relevant guidance issued by Ofcom. We set out in the table below our initial view of the thresholds at which NIS incidents will have a significant impact and they should therefore be reported to Ofcom.

4.49 We will in due course discuss these initial thresholds with DCMS, the NCSC and individual OES as they identify themselves to us. We expect that we might need to refine them based on these discussions in any revised guidance.

4.50 We understand that putting in place processes to ensure qualifying incidents are reliably reported is likely to take some time for the OES. Meanwhile, we would encourage all the designated OES to make their best efforts to report relevant incidents. We would expect that they will not adopt an unduly restrictive approach to interpreting these criteria – our general guidance is that, if there is any doubt as to whether (or not) a criterion is met, the OES should submit a report to Ofcom

Table of specific reporting thresholds

Digital Infrastructure OES	Customer / Volume Based Approach	Service Degradation
DNS TLD	**Loss or significant degradation of >= 50% of name resolution capability**	**1 hour**
DNS Public Resolver	**Loss or significant degradation of service to >= 50% of clients**	**30 minutes**
DNS Authoritative Hosting	**Loss or significant degradation (e.g. serving incorrect results) of service for >=50% of domains**	**1 hour**
IXP	**Loss or significant degradation of connectivity to 25% of connected global routes**	**1 hour**
	Loss of >= 90% of total port capacity	

5. Ofcom's approach to enforcement

Ofcom's interim approach to enforcement

5.1 Ofcom's approach to our enforcement in cases relating to electronic communications networks and services and postal services, and some cases relating to breaches of wireless telegraphy licences is set out in our publication Enforcement guidelines for regulatory investigations[8]. We expect our approach to enforcement of the NIS Regulations to be broadly in line with those Enforcement guidelines. Our enforcement approach might, however, have to be adapted to reflect specific requirements concerning enforcement in Parts 5 and 6 of the NIS Regulations. We will in due course consider whether there is a need to review the application of those Enforcement guidelines to our enforcement under the NIS Regulations, and DCMS' implementation guidance to CAs.

5.2 We are aware that the NIS Regulations represent entirely new duties for many of the designated OES in scope. For some of them, this may be the first time they have been subject to any security regulation, or any regulation enforced by Ofcom. We are always required to take a proportionate approach to any regulations that we enforce and will do so also in relation to the NIS Regulations. This is also reflected in regulation 23(1) of the NIS Regulations.

5.3 In relation to managing security risks, there should always be a continuous process of evaluating current risks and making appropriate changes to security measures as a result. Many designated OES will therefore be undertaking an ongoing process of security improvement, for some perhaps triggered or heightened by the introduction of the NIS Regulations. We understand that it will take time for them to understand the practical application of their duties under the NIS Regulations, and that any required security improvements might take time to achieve, and ongoing effort to maintain.

5.4 As mentioned above, we expect that the NCSC will shortly issue its CAF. We will review this in detail when it is available, alongside the NIS Regulations. It is our expectation that the CAF will be an important tool in our assessment of an OES' compliance with their duties under the NIS Regulations. We may determine that we need to supplement or modify some aspects in order to fully address the particular needs of the digital infrastructure subsector. We note that, while the CAF will be focused on cyber security issues, many of the objectives and controls it will cover will also be relevant to non-cyber security.

5.5 Our current view is that we may ask designated OES to assess themselves against the CAF in the last quarter of 2018. This would form part of our initial assessment of the compliance of the sector and help identify any areas where additional work is required. Such an approach would be in line with our understanding of Government's NIS implementation guidance to Competent Authorities.

[8] https://www.ofcom.org.uk/__data/assets/pdf_file/0015/102516/Enforcement-guidelines-for-regulatory-investigations.pdf

Ofcom's powers of inspection

5.6 Ofcom has the power under regulation 16 to conduct itself or commission an inspection of designated OES in order to assess if it has fulfilled its duties under regulations 10 and 11 of the NIS Regulations

5.7 For the purposes of carrying out the inspection, the designated OES is under a duty to:

- pay the reasonable costs of the inspection;
- co-operate with the person who is conducting the inspection ("the inspector");
- provide the inspector with reasonable access to their premises;
- allow the inspector to inspect, copy or remove such documents and information, including information that is held electronically, as the inspector considers to be relevant to the inspection; and
- allow the inspector access to any person from whom the inspector seeks relevant information for the purposes of the inspection.

Penalties

5.8 Ofcom has the power under regulation 18 to impose penalties in certain circumstances. The amounts of any penalties imposed are subject to maximum limits laid down in regulation 18(6).

5.9 Section 392 of the Communications Act 2003 requires Ofcom to prepare and publish a statement containing the guidelines it proposes to follow in determining the amount of penalties imposed by Ofcom under the Act or any other enactment apart from the Competition Act 1998. The NIS Regulations constitute such other enactment.

5.10 By virtue of section 392(6) of that Act, Ofcom must have regard to the statement for the time being in force when setting the amount of any penalty under this Act or any other enactment (apart from the Competition Act 1998). Our current guidelines are set out in Ofcom's statement containing the penalty guidelines[9].

Independent review of designation decisions and penalty decisions

5.11 Regulation 19 of the NIS Regulations makes, in effect, provision for independent reviews of Ofcom's designation decisions and penalty decisions. If an OES so requests, we must appoint an independent person to conduct reviews of such decisions.

5.12 We are not in a position at this stage to give any details about how this process might work in relation to any such decisions taken by Ofcom, taking into account all of the requirements of regulation 19. We will in due course give further consideration to this matter, especially if we would be minded to designate any OES or impose any penalties.

[9] https://www.ofcom.org.uk/__data/assets/pdf_file/0022/106267/Penalty-Guidelines-September-2017.pdf

A1. Reference URLs

Statutory Instrument: http://www.legislation.gov.uk/uksi/2018/506/pdfs/uksi_20180506_en.pdf

NCSC NIS Guidance Collection: https://www.ncsc.gov.uk/guidance/nis-guidance-collection

A2. Contact the Ofcom NISD team

Email nis@ofcom.org.uk for general enquiries.

Email incident@ofcom.org.uk with incident reports.