Ofcom
making communications work
for everyone

Guidance for the digital infrastructure subsector

Statutory guidance under the Network and Information Systems Regulations 2018: NIS Guidance

GUIDANCE

Publication Date: 5 February 2021

About this document

Ofcom is the designated competent authority for the digital infrastructure subsector in the United Kingdom under the Network and Information Systems (NIS) Regulations 2018. We must prepare and publish guidance in relation to that subsector under the NIS Regulations.

This statutory guidance sets out how we normally would expect to approach our functions under the NIS Regulations and will be of primary interest to those operators of essential services (OES) that we regulate under the digital infrastructure subsector. This guidance includes:

- matters relevant to identification and designation of OES, including:
    - how persons "deemed" to be OES under the NIS Regulations must notify Ofcom;
    - how non-UK based OES must notify Ofcom regarding their nominated person authorised to act on their behalf in the UK;
- matters to which OES must have regard in complying with their security duties and duties to notify NIS incidents to Ofcom, including the process, format and thresholds for their reporting, imposed on OES under the NIS Regulations;
- how Ofcom will investigate compliance with, and approach enforcement of requirements imposed under the NIS Regulations;
- details of the appeal process that applies to our appealable decisions; and
- how Ofcom will recover from OES our reasonable costs in carrying out relevant functions under the NIS Regulations.

Contents

Section

Annexes

1. Introduction

What this Guidance covers

1.1 Ofcom is the designated competent authority for the digital infrastructure subsector in the United Kingdom for the Network and Information Systems Regulations 2018[1] (more commonly referred to simply as the "NIS Regulations"). They were made on 19 April 2018 and came into force on 10 May 2018.

1.2 We must prepare and publish statutory guidance in relation to that subsector under the NIS Regulations.[2] In particular, we may publish guidance to deal with matters to which so-called operators of essential services ("OES") must have regard to in complying with their security duties[3] and also their separate duties to notify NIS incidents to Ofcom.[4]

1.3 On 8 May 2018, we published our initial (interim) guidance for those purposes ("Ofcom's Interim NIS Guidance").[5] This Guidance replaces Ofcom's Interim NIS Guidance with immediate effect. Annex A5 sets out a version history of this Guidance.

1.4 On 5 November 2020, the Secretary of State made regulations to amend the NIS Regulations, namely the Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020.[6] Those amendments came into force on 31 December 2020. We refer throughout this Guidance to the NIS Regulations amended by those 2020 Regulations as the "Amended NIS Regulations".[7]

1.5 The Amended NIS Regulations introduce some important changes that we consider should be reflected in this updated Guidance.

Role and evolution of this Guidance

1.6 Guidance has the benefit of contributing to effective regulation by improving transparency and understanding. This Guidance is particularly aimed at encouraging OES' compliance with their duties under the Amended NIS Regulations concerning matters such as:

---

[1] S.I. 2018/506 as amended by S.I. 2018/629. They 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] Regulation 3(3)(b).
[3] Regulation 10(4).
[4] Regulation 11(12).
[5] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/guidance-network-information-systems-regulations
[6] S.I. 2020/1245.
[7] The NIS Regulations have also been amended by the Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019/653) and the Network and Information Systems (Amendment etc.) (EU Exit) (No. 2) Regulations 2019 (SI 2019/1444). Those amendments were initially stated as coming into force on the twentieth day after "exit day". However, paragraph 1 of Schedule 5 to the European Union (Withdrawal Agreement) Act 2020 has changed that commencement date, so that the reference to "exit day" is to be read instead as a reference to "IP completion day", which means 31 December 2020 at 11.00 pm (see section 39(1) of that Act). Accordingly, those amendments to the NIS Regulations came into force on 20 January 2021.

- identification and designations of OES under regulation 8;
- OES' security measures under regulation 10; and
- OES' NIS incident notifications to us under regulation 11.

1.7 One of our regulatory principles is that we will regulate in a transparent manner[8]. Guidance can serve as a useful means to achieving this principle and to increasing understanding of our policy objectives and approach to regulation.

1.8 Furthermore, we have already explained above that we must prepare and publish statutory guidance in relation to the digital infrastructure subsector under regulation 3(3)(b) of the Amended NIS Regulations. This Guidance therefore deals with additional matters relevant to our functions under the Amended NIS Regulations:

- our information sharing powers;
- our information gathering powers;
- our powers of inspection;
- our approach to enforcement action;
- details of the appeal process for relevant decisions; and
- our approach to cost recovery.

1.9 We anticipate that we will need to update this Guidance from time to time, especially as we gain a better understanding of the digital infrastructure subsector. Matters on which we may give further guidance could also arise from (for example) us engaging with OES and others affected by their essential services. We also anticipate our continued dialogue with the National Cyber Security Centre[9] ("NCSC"), the Department of Digital, Culture, Media & Sport ("DCMS") and other regulators about matters relevant to the Amended NIS Regulations, which may result in the need for us to update this Guidance.

1.10 Should you wish to contact Ofcom's NIS team regarding this Guidance, please use our contact details set out in Annex A1.

Status of this Guidance

1.11 This Guidance sets out how we normally would expect to approach our functions under the Amended NIS Regulations. However, we cannot, as a matter of law, fetter our discretion as to any future decision. Accordingly, although this Guidance sets out our normal expected approach, it does not have binding legal effect, and we may depart from it if we consider it appropriate in the circumstances of a particular case. If we were to depart from this Guidance, we will set out our reasons for doing so.

1.12 Additionally, this Guidance is neither a substitute for any regulation or law, nor does it represent legal advice. Whether or not (and, if so, how) a matter is regulated will usually turn on the specific facts in each case. Therefore, you should always seek your own independent advice on specific matters, considering the facts in question to answer

[8] https://www.ofcom.org.uk/__data/assets/pdf_file/0020/42770/ch2.pdf
[9] https://www.ncsc.gov.uk/

specific questions on duties imposed under the Amended NIS Regulations, together with other relevant matters.

The UK national framework under the Amended NIS Regulations

The UK Government's NIS national strategy

1.13 The national framework under the Amended NIS Regulations is set by the Government. It must publish a strategy to provide strategic objectives and priorities on the security of network and information systems in the United Kingdom (the "NIS national strategy"). [10]

1.14 The strategic objectives and priorities set out in the NIS national strategy must be aimed at achieving and maintaining a high level of security of network and information systems in the sectors (as well as digital services) regulated by various regulators under the Amended NIS Regulations. It must, in particular, address the following matters:

- the regulatory measures and enforcement framework to secure the objectives and priorities of the strategy;
- the roles and responsibilities of the key persons responsible for implementing the strategy;
- the measures relating to preparedness for, response to and recovery from incidents, including cooperation between public and private sectors;
- education, awareness-raising and training programmes relating to the strategy;
- research and development plans relating to the strategy;
- a risk assessment plan identifying any risks; and
- a list of the persons involved in the implementation of the strategy.

1.15 Ofcom must have regard to the NIS national strategy when carrying out its duties under the Amended NIS Regulations.[11] We also recommend that OES themselves have regard to the NIS national strategy when planning, implementing, monitoring or updating any technical and organisational security measures they take in order to comply with their duties under the Amended NIS Regulations (which duties we further detail in Section 5 of this Guidance).

Supervisory authorities as part of the UK national framework

1.16 The UK national framework under the Amended NIS Regulations seeks 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.

---

[10] Regulation 2(1) of the Amended NIS Regulations. We understand that the NIS national strategy covering the 5-year period between 2016 and 2021 is set out in the Government's plan to make Britain secure and resilient in cyberspace, which is contained in its document entitled 'National Cyber Security Strategy 2016 to 2021', published on 1 November 2016:
'https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[11] Regulation 3(6).

1.17 In doing so, the establishment of the following supervisory authorities plays a role:

- relevant law-enforcement authorities;[12]
- designated competent authorities other than Ofcom (i.e. regulators) for their respective subsectors[13] in relation to which OES provide essential services;
- a Single Point of Contact ("SPOC") on the security of network and information systems for the United Kingdom;[14] and
- a Computer Security Incident Response Team ("CSIRT") for the United Kingdom in respect of the relevant sectors and digital services.[15]

The NCSC's roles under the Amended NIS Regulations

1.18 The National Cyber Security Centre (NCSC) is part of the Government Communications Headquarters (GCHQ) and, as such, provides technical support and guidance to other government departments, devolved administrations, competent authorities and OES.

1.19 In particular, the NCSC carries out, in practice, the following three different roles under the national framework described above:

- **SPOC role** – GCHQ (the NCSC) may consult and co-operate with relevant law enforcement authorities, and also with the NIS enforcement authorities to enable them to fulfil their obligations under the Amended NIS Regulations. The NCSC may also liaise with the relevant authorities in any Member State of the EU, the Cooperation Group[16] and the CSIRTs' network[17]. Additionally, the NCSC may submit incident reports to the Cooperation Group and reports to the European Commission on identified OES.
- **CSIRT role** – GCHQ (the NCSC) discharges various obligations set out in regulation 5 of the Amended NIS Regulations, such as monitoring incidents in the United Kingdom.
- **Advisory role** – as noted above, the NCSC provides support to OES (as well as to competent authorities like Ofcom) with cyber security advice and guidance and it also acts as a source of technical expertise. The NCSC CAF Guidance[18] brings together advice published by the NCSC that is relevant to OES and reflects indicators of good practice.

[12] A "relevant law-enforcement authority" has the meaning given in section 63A(1A) of the Police and Criminal Evidence Act 1984, such as a police force and the National Crime Agency.
[13] The sectors are: (i) Energy (i.e. electricity, oil and gas); (ii) Transport (i.e. air, rail, water and road transport); (iii) Health (i.e. health care settings including hospitals, private clinics and online settings); and (iv) Drinking water supply and distribution. The designated competent authorities for those subsectors are specified in Column 3 of the table in Schedule 1 to the Amended NIS Regulations.
[14] Regulation 4 designates Government Communications Headquarters ("GCHQ") as the SPOC.
[15] Regulation 5 designates GCHQ also as the CSIRT.
[16] "Cooperation Group" means the group established under Article 11(1) of the NIS Directive.
[17] "CSIRTs network" means the network established under Article 12(1) of the NIS Directive.
[18] https://www.ncsc.gov.uk/collection/caf. In summary, it sets out: (i) 4 top-level security objectives; (ii) a set of sector-agnostic Security Principles which support the delivery of those objectives, each principle describing security outcomes to be achieved; and (iii) a Cyber Assessment Framework ("CAF") incorporating indicators of good practice.

Glossary

1.20 We set out in Annex A3 a glossary of abbreviations and acronyms we use throughout this Guidance.

2. Our role for the digital infrastructure subsector

Our designation for the digital infrastructure subsector

2.1 Ofcom is specified in column 3 of the table in Schedule 1 to the Amended NIS Regulations as the "competent authority" for the "digital infrastructure subsector" and for the whole territorial jurisdiction of the United Kingdom.

2.2 As such, Ofcom is a regulator designated under regulation 3(1) of the Amended NIS Regulations. As regards that territorial jurisdiction, it should also be noted that regulation 1(6) of the Amended NIS Regulations states that they apply to the United Kingdom (including its internal waters) and the territorial sea adjacent to the United Kingdom.

Meaning of this subsector

2.3 The notion of the "digital infrastructure subsector" has not been defined as such under the Amended NIS Regulations. However, the types of essential services falling within that subsector (and corresponding regulated OES[19]) are:

Essential Service	**OES[20]**
Top Level Domain **("TLD")** Name Registry	TLD Name Registry
Domain Name System **("DNS")** Resolver Service	DNS Service Provider
DNS Authoritative Hosting Service	DNS Service Provider
Internet Exchange Point **("IXP")**	IXP Operator

Our main duties in relation to this subsector

2.4 In relation to the digital infrastructure subsector, we must do the following things:[21]

a) periodically review the application of the Amended NIS Regulations in conjunction with DCMS and others;

b) prepare and publish guidance in such form and manner as we consider appropriate. Such guidance may be reviewed at any time and any revised guidance must be published as soon as reasonably practicable;

[19] An "OES" ("operator of an essential service") means a person who is deemed to be designated as an operator of an essential service under regulation 8(1) or is designated as an operator of an essential service under regulation 8(3) of the Amended NIS Regulations. We further detail OES designations in the digital infrastructure subsector in Section 4 of this Guidance.

[20] A person is only deemed to be designated as an OES for the digital infrastructure subsector, if certain threshold requirements are met, which we detail in Section 4 of this Guidance.

[21] These requirements are imposed on Ofcom under regulation 3(3) of the Amended NIS Regulations.

c) keep a list of all the OES who are designated, or deemed to be designated, under regulation 8;

d) keep a list of all the OES revocations made under regulation 9;

e) send a copy of each of those lists to the SPOC to enable it to prepare the report mentioned in regulation 4(3);

f) consult and co-operate with the Information Commissioner when addressing incidents that result in breaches of personal data; and

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

i. relevant law-enforcement authorities;
ii. other competent authorities in the UK;
iii. the SPOC; and
iv. the CSIRT.

2.5 We may also consult and co-operate with a public authority in the EU if it is in the interests of effective regulation of the digital infrastructure subsector (whether inside or outside the United Kingdom).[22]

Our powers in relation to this subsector

2.6 As the designated competent authority for the digital infrastructure subsector, we have various powers under the Amended NIS Regulations. In particular, we may:

- designate someone as an OES[23] (even if a person does not meet relevant threshold requirements provided certain conditions are met), and we may also revoke OES designations under certain circumstances[24] – see further in Section 4 of this Guidance;
- publish guidance that OES must have regard to when carrying out their duties imposed by regulations 10 and 11 – see further in Section 5 of this Guidance;
- share information with other NIS enforcement authorities, relevant law-enforcement authorities, the CSIRT, and public authorities in the EU under certain circumstances[25] – see further in Section 6 of this Guidance;
- gather information by serving information notices – see further in Section 7 of this Guidance;
- conduct inspections – see further in Section 8 of this Guidance;
- take enforcement action – see further in Section 9 of this Guidance; and
- recover from OES our reasonable costs in carrying out relevant NIS functions – see further in Section 11 of this Guidance.

[22] See paragraph 4(c) of the Schedule to the Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019/653), which came into force on 20 January 2021 (see footnote 7 above).
[23] Regulation 8(3).
[24] Regulation 9.
[25] Regulation 6.

3. Our general duties

Our principal duty

3.1 Section 3 of the Communications Act 2003 imposes general duties on Ofcom when we carry out our functions conferred on us by or under any enactment, including under the Amended NIS Regulations.

3.2 Specifically, section 3(1) provides that it is our principal duty to further the interests of citizens in relation to communications matters (i.e. matters in relation to which we have functions), and to further the interests of consumers in relevant markets, where appropriate by promoting competition.

Statutory factors in performing our general duties

3.3 In performing our general duties, we must have regard, in all cases, to:[26]

- 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 us to represent the best regulatory practice.

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

Our relevant considerations

3.5 We will secure or further the performance of our general duties by or in relation to what we do in carrying out our functions under the Amended NIS Regulations. In doing so, we will have regard to any other relevant matters, such as the NIS national strategy that we note in Section 1 of this Guidance.

3.6 For example, taking action in respect of non-compliance with the statutory requirements and duties imposed on OES under the Amended NIS Regulations is usually likely to further the interests of citizens and consumers by preventing or remedying consumer harm.

3.7 Such action is also likely to achieve and maintain a high level of security of network and information systems in the digital infrastructure subsector, in line with the strategic objectives and priorities set out in the NIS national strategy. However, before we take such action, we must also consider whether it is reasonable and proportionate, on the facts and circumstances of the case[27]. As noted above, our enforcement action should also be targeted only at cases in which action is needed under section 3(3) of the Communications Act 2003.

[26] Section 3(3) of the Communications Act 2003.
[27] Regulation 23 of the Amended NIS Regulations.

4. OES designations for the digital infrastructure subsector

Meaning of OES

4.1 The concept of "OES" (or "operator of an essential service") means, for the purposes of the Amended NIS Regulations, "*a person who is deemed to be designated as an operator of an essential service under regulation 8(1) or is designated as an operator of an essential service under regulation 8(3)*".[28]

4.2 In this section, we explain:

- firstly, the categories of persons who are deemed to be designated as OES;
- secondly, our powers to designate additional persons as OES;
- thirdly, OES' duties to notify Ofcom of their deemed OES designations and any change in circumstances affecting their OES designations;
- fourthly, our powers to revoke any OES designations;
- fifthly, the duties of non-UK based OES to notify Ofcom of their appointment of a nominated person; and
- sixthly, our administration of OES designations.

OES "deemed to be designated" for this subsector

Who are "deemed" OES for this subsector

4.3 Regulation 8(1) of the Amended NIS Regulations "deems" certain persons as designated OES for the digital infrastructure subsector. Importantly, such deemed designations apply automatically by operation of law laid down in regulation 8(1), without the need for Ofcom to take any decision to designate them as such, nor is it necessary for Ofcom to contact an OES for it to be deemed as an OES. This is because regulation 8(1) provides that:

[28] Regulation 1(2).

> *"8.— (1) If a person[29] provides an essential service of a kind referred to in 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.*"

4.4 However, regulation 8(1) does not apply to a network provider or service provider who is subject to the requirements of sections 105A to 105C of the Communications Act 2003.[30] We deal below with certain DNS Resolver Services in relation to which this exception is relevant.

4.5 As regards the reference in regulation 8(1) to "*an essential service **of a kind referred to in Schedule 2***" (emphasis added), we have already introduced in Section 2 of this Guidance the types of essential services falling within the digital infrastructure subsector. We deal in detail below with the various categories of such essential services. They are described in paragraph 10 of Schedule 2 to the Amended NIS Regulations for the digital infrastructure subsector, which paragraph also describes the associated threshold requirements.

4.6 For the avoidance of doubt, it is possible that a person could be deemed to be designated as an OES for more than one of those categories. For example, an organisation that provides both DNS Resolver Services as well as DNS Authoritative Hosting Services would, if the relevant threshold requirements are met in both cases, be deemed to be designated as an OES for each such essential service.

Definitional issues

4.7 The application of regulation 8(1) requires consideration of various defined concepts.

4.8 It should firstly be noted that:

> "*"essential service" means a service which is essential for the maintenance of critical societal or economic activities;*"[31]

4.9 Regulation 8(1) also requires that such an essential service "*relies on network and information systems*". In that regard, it should be noted that:

---

[29] The word "person" is here used in a legal sense. It could be used to describe a human being as well as another type of person, such as a corporation or a partnership. This is because Schedule 1 to the Interpretation Act 1978—which applies to the interpretation of the Amended NIS Regulations—provides that a 'person' includes a body of persons corporate or unincorporate.

[30] Regulation 8(1A). The concepts of "network provider" and "service provider" have the meanings given in section 105A(5) of the Communications Act 2003, namely: "network provider" means a provider of a public electronic communications network, and "service provider" means a provider of a public electronic communications service.

[31] Regulation 1(2).

> *"'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;"* [32]

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

> *"(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.*"

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

- "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));
- "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)); and
- "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)).

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

4.13 A "signal" includes anything comprising speech, music, sounds, visual images or communications or data of any description; and signals serving for the impartation of

[32] Regulation 1(2).

anything between persons, between a person and a thing or between things, or for the actuation or control of apparatus (section 32(10)).

Overseas (non-UK) establishment

4.14 Prior to the Amended NIS Regulations, the threshold requirements for DNS service providers providing a DNS Resolver Service or DNS Authoritative Hosting Service included a requirement that such providers needed an establishment in the United Kingdom.

4.15 This requirement has been removed by the Amended NIS Regulations. The threshold requirements for the digital infrastructure subsector now apply irrespectively of place of establishment (whether within, or outside of, the United Kingdom).

4.16 Linked to that change, regulation 8A imposes a new duty[33] on OES for the digital infrastructure subsector, who have their head offices outside the United Kingdom, to notify Ofcom of a person in the United Kingdom with the authority to act on their behalf under the Amended NIS Regulations, including for the service of documents for the purposes of regulation 24 (a "nominated person"). We note below how (and what details) non-UK based OES must notify Ofcom in relation to their nominated persons.

First category of deemed OES: Top Level Domain Name Registries (TLD)

4.17 As already noted above, paragraph 10 of Schedule 2 to the Amended NIS Regulations describes the threshold requirements which apply to specified kinds of essential services in the digital infrastructure subsector.

4.18 The first category[34] of such essential services deemed to be designated as an OES is the following essential service:

> "*For the essential service of **a TLD Name Registry**, **irrespective of its place of establishment** (whether within, or outside of, the United Kingdom), the threshold in the United Kingdom is a TLD Name Registry which services **14 billion or more queries from any devices located within the United Kingdom in any consecutive 168-hour period for domains registered within the Internet Corporation for Assigned Names and Numbers** ("ICANN").*" (emphasis added)

4.19 In that regard, it should be noted that "TLD Name Registry" is a reference to "Top-Level Domain Name Registry", meaning an entity which administers and operates the registration of internet domain names under top-level domains.[35]

4.20 We expect that devices located within the United Kingdom would normally be identified, for example, through:

---

[33] On 4 January 2021, we published an interim Update Note to explain, in particular, how non-UK based OES should their nominated persons to Ofcom - https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/guidance-network-information-systems-regulations This Guidance replaces that interim Update Note with immediate effect.

[34] Paragraph 10(2) of Schedule 2 to the Amended NIS Regulations.

[35] Paragraph 10(5)(d) of Schedule 2 to the Amended NIS Regulations.

- examining if the source IP address is officially assigned to UK based entities (whether to legal persons or human beings) by a Regional Internet Registry (RIR);
- examining if the source IP address is allocated to UK based providers of public electronic communications networks and services;
- examining the source networks of queries, and determining if this is a UK based provider of public electronic communications networks and services; or
- by aggregating queries deemed to come from UK based sources.

Second category of deemed OES: Domain Name Service Providers (DNS)

DNS Service Providers

4.21 The second category of essential services deemed to be designated as an OES for the digital infrastructure subsector relates to specific services provided by DNS service providers. There are, in fact, two sub-categories of such essential services, which we detail below.

4.22 Common to both sub-categories are the following definitions:[36]

> (a) "DNS" is a reference to “Domain Name System” which means a hierarchical distributed naming system which processes and responds to queries for DNS resolution;
>
> (b) "DNS service provider" is a reference to "Domain Name System service provider" which means an entity which provides DNS services accessible via the internet;

First sub-category: DNS Resolver Services

4.23 The first sub-category[37] of this second category of essential services deemed to be designated as an OES is the following kind of essential service:

> *“For the essential service of **a DNS resolver service** provided by a DNS service provider, **irrespective of its place of establishment** (whether within, or outside of, the United Kingdom), the threshold in the United Kingdom is a DNS resolver service **which services 500,000 or more different Internet Protocol addresses used by persons in the United Kingdom in any consecutive 168-hour period.**”* (emphasis added)

4.24 The concept of a “DNS resolver service” is not defined in the Amended NIS Regulations. In simple terms, a DNS Resolver Service is a service providing responses to DNS queries which may come from its own database, or from other DNS databases, for example, from DNS TLD Name Registries, DNS Authoritative Hosting Services or other databases of DNS information.

[36] Paragraph 10(5)(a) and (b) of Schedule 2 to the Amended NIS Regulations.
[37] Paragraph 10(3) of Schedule 2 to the Amended NIS Regulations.

Potential regulatory overlap for DNS Resolver Services

4.25 We have noted above that regulation 8(1) does not apply to a network provider or service provider who is subject to the requirements of sections 105A to 105C of the Communications Act 2003.

4.26 In November 2018, we gave specific guidance to some Internet Service Providers (ISPs) on matters to be taken into account in considering any overlap between the (initial) NIS Regulations and the section 105A regime in relation to DNS Resolvers Services. We have included that specific guidance in Annex A4, which guidance we consider remains relevant under the Amended NIS Regulations.

Second sub-category: DNS Authoritative Hosting Services

4.27 The second sub-category[38] of this second category of essential services deemed to be designated as an OES is the following kind of essential service:

> "*For the essential service of **a DNS authoritative hosting service** provided by a DNS service provider, **irrespective of its place of establishment** (whether within, or outside of, the United Kingdom), the threshold in the United Kingdom is a DNS authoritative hosting service **which services 100,000 or more domains registered to persons with an address in the United Kingdom.***" (emphasis added)

4.28 The concept of a "DNS authoritative hosting service" is not defined in the Amended NIS Regulations. In simple terms, a DNS Authoritative Hosting Service typically provides storage, maintenance and access to DNS information ('DNS Records') associated with a particular DNS domain. Such hosting services are typically accessed by DNS Resolver Services, which request information from the hosting service as needed, on behalf of the consumers of the DNS Resolver Service.

Third category of deemed OES: Internet Exchange Point Operators (IXP)

4.29 The third[39] category of essential services deemed to be designated as an OES for the digital infrastructure subsector is the following kind of essential service:

> "*For the essential service of an IXP provided by an IXP operator, irrespective of its place of establishment (whether within, or outside of, the United Kingdom), the threshold in the United Kingdom is **an IXP operator which has 30% or more market share amongst IXP operators in the United Kingdom, in terms of interconnected autonomous systems.***" (emphasis added)

4.30 In that regard, the following definitions[40] should be noted:

---

[38] Paragraph 10(3A) of Schedule 2 to the Amended NIS Regulations.
[39] Paragraph 10(4) of Schedule 2 to the Amended NIS Regulations.
[40] Paragraph 10(5)(c) and (ca) of Schedule 2 to the Amended NIS Regulations.

> "*(c) "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; and*
>
> *(ca) "IXP Operator" means a person who provides an IXP to another person and, where one or more persons are employed or engaged to provide an IXP under the direction or control of another person, it means only that other person.*"

Statutory duty to notify us about "deemed" OES designations

What OES duties are

4.31 Regulation 8(2) of the Amended NIS Regulations imposes the following statutory duty on OES falling within the digital infrastructure subsector:

> "*(2) A person who falls within paragraph (1) must notify the designated competent authority in writing of that fact before the notification date.*"

Deadline for notifying Ofcom

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

> "*(a) 10th August 2018, in the case of a person who falls within paragraph (1) on the date these Regulations come into force; or*
>
> *(b) in any other case,* ***the date three months after the date on which the person falls within that paragraph****.*" (emphasis added)

4.33 The Amended NIS Regulations have introduced some important changes to the threshold requirements which apply to the kinds of essential services falling within the digital infrastructure subsector. Those changes came into force on 31 December 2020.

4.34 This means for example that, if any person was deemed to be designated as an OES under regulation 8(1) at the time those changed threshold requirements came into force (i.e. on 31 December 2020), such a person must notify Ofcom in writing of that fact (i.e. that the person is deemed to be designated as an OES under regulation 8(1)) by 31 March 2021.

4.35 Alternatively, if a person did not fall with regulation 8(1) on 31 December 2020 but subsequently does so, such a person must notify Ofcom in writing of that fact within 3 months of coming into scope.

How to notify Ofcom of the "deemed" designation as an OES

4.36 Any person to whom the notification duty under regulation 8(1) applies must notify Ofcom in the following manner:

- send an email to nis@ofcom.org.uk;
- in the subject line of that email, state 'NIS designation notification';
- state clearly in your email which above-mentioned category (or, as the case may be, categories) of deemed OES you fall into; for DNS Service Providers, they must specify which above-mentioned sub-category (or, as the case may be, sub-categories) they fall into; and
- provide your contact details, together with (where relevant) company details of the person about whom you are notifying as a deemed OES including full registered company name, trading name (if any), registered office address, and registered company number.

Consequences of failure to notify us

4.37 Any failure to comply with the notification duty under regulation 8(1) may be enforced by Ofcom under regulation 17 and we may also impose penalties under regulation 18 in relation to such a failure (see Section 9 of this Guidance).

Our powers to designate additional persons as OES

What our powers are

4.38 Even if a person does not meet the threshold requirements for a specific category of OES set out in the Amended NIS Regulations (as noted above), we have the power under regulation 8(3) to designate such a person as an OES for the digital infrastructure subsector.

4.39 However, we can only designate another person as an OES if the following three conditions are met:

- first, that person provides an essential service of a kind specified in paragraph 10 of Schedule 2 to the Amended NIS Regulations for the digital infrastructure subsector;
- second, the provision of that essential service by that person relies on network and information systems; and
- third, we conclude that an incident affecting the provision of that essential service by that person is likely to have significant disruptive effects on the provision of the essential service.

4.40 In order to arrive at our conclusion concerning the likelihood of significant disruptive effects, we must have regard to the following eight factors:[41]

- the number of users relying on the service provided by the person;

[41] Regulation 8(4).

- the degree of dependency of the other relevant sectors on the service provided by that person;
- the likely impact of incidents on the essential service provided by that person, in terms of its degree and duration, on economic and societal activities or public safety;
- the market share of the essential service provided by that person;
- the geographical area that may be affected if an incident impacts on the service provided by that person;
- the importance of the provision of the service by that person 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 by that person; and
- any other factor we consider appropriate to have regard to, in order to arrive at the above-mentioned conclusion.

How we would exercise our designation powers

4.41 Before we designate any person as an OES, we may invite the person to submit any written representations about our proposed decision to designate it as an OES.

4.42 We normally expect to use our information gathering powers (see Section 7 of this Guidance), when we are assessing whether a person should be an OES, particularly to establish whether the conditions in regulation 8(3) are met.

4.43 The way in which we would designate an OES is by means of a notice in writing served on the person who is to be designated in accordance with regulation 24 of the Amended NIS Regulations and providing our reasons for the designation in that notice.[42]

4.44 Our decision under regulation 8(3) to designate a person as an OES may be appealed under regulation 19A(1)(a) of the Amended NIS Regulations (see Section 10 of this Guidance).

OES duties to notify us about changes affecting OES designations

What OES duties are

4.45 Regulation 8(7A) imposes a statutory duty in that, if a person has reasonable grounds to believe that it no longer falls within regulation 8(1) or that the conditions for designation under regulation 8(3) are no longer met in relation to that person, such a person must as soon as practicable notify Ofcom in writing and provide with that notification evidence supporting that belief.

4.46 Where we receive from a person a notification and supporting evidence referred to in regulation 8(7A), we must have regard to that notification and evidence in considering whether to revoke that person's designation.

[42] Regulation 8(5).

How to notify us of change in circumstances affecting OES designations

4.47 Any person to whom the notification duty under regulation 8(7A) applies must notify Ofcom in the following manner:

- send an email to nis@ofcom.org.uk;
- in the subject line of that email, state 'NIS designation notification – change in circumstances';
- state clearly in your email which above-mentioned category (or, as the case may be, categories) of deemed OES you fall into and in relation to which your circumstances have changed affecting your OES designation; for DNS Service Providers, they must specify which above-mentioned sub-category (or, as the case may be, sub-categories) is affected in that regard;
- provide detailed reasons in support of your belief why you have reasonable grounds to believe that you no longer fall within regulation 8(1) or that the conditions for designation under regulation 8(3) are no longer met;
- provide your evidence in support of that belief; and
- provide your contact details, together with (where relevant) company details of the person about whom you are notifying the above-mentioned change in circumstances including full registered company name, trading name (if any), registered office address, and registered company number.

Our powers to revoke OES designations

What our powers are

4.48 We have the power under regulation 9(1) to revoke a deemed OES designation falling under regulation 8(1) by serving a notice in writing, 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 factors mentioned in regulation 8(4).[43]

4.49 We may 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.

How we would exercise our revocation powers

4.50 Before revoking a deemed designation of a person as an OES under regulation 8(1) or a designation of a person as an OES under regulation 8(3), we must:[44]

- serve a notice in writing of our proposed revocation on that person;
- provide reasons for our proposed decision;

[43] Regulation 9(4). See paragraph 4.40 above for the eight factors mentioned in regulation 8(4).
[44] Regulation 9(3).

- invite that person to submit any written representations about our proposed decision within such time period as may be specified by us; and
- consider any representations submitted by that person before we take our final decision to revoke the designation.

4.51 The way in which we would then finally revoke an OES designation is by means of a notice in writing served on the person who is affected by our final decision to revoke the designation in accordance with regulation 24 of the Amended NIS Regulations.

4.52 Our decision under regulation 9(1) or (2) to revoke the designation may be appealed under regulation 19A(1)(b) of the Amended NIS Regulations (see Section 10 of this Guidance).

Appointment of a nominated person by a non-UK based OES

Overseas (non-UK) establishment of OES in this subsector

4.53 We have already mentioned earlier in this section that the threshold requirements for the digital infrastructure subsector now apply irrespectively of place of establishment (whether within, or outside of, the United Kingdom).

4.54 Some OES falling within this subsector may have their head offices outside of the United Kingdom. Indeed, they may not even have a physical presence in the United Kingdom in providing the essential services in relation to which they have been designated as an OES.

What OES duties are

4.55 Regulation 8A(3) imposes a statutory duty in that any OES for the digital infrastructure subsector, who have their head offices outside the United Kingdom[45], must notify Ofcom of a person in the United Kingdom with the authority to act on their behalf under the Amended NIS Regulations, including for the service of documents for the purposes of regulation 24 (a "nominated person").

4.56 An OES to whom regulation 8A(1) applies must notify Ofcom in writing before the "relevant date" of:

- their name;
- the name and address of the nominated person; and
- up-to-date contact details of the nominated person (including email addresses and telephone numbers).

4.57 The concept of "relevant date" is defined in regulation 8A(7) as:

[45] Regulation 8A(1).

> *"(7) In this regulation, "relevant date" means the date three months after—*
>
> *(a) the first day (including that day) on which the OES was deemed to be designated as an OES under regulation 8(1); or*
>
> *(b) the day (including that day) on which the OES was designated as an OES under regulation 8(3),*
>
> *unless the first day referred to in sub-paragraph (a) or the day referred to in sub-paragraph (b) was before 31st December 2020 in which case it means 31st March 2021."*

4.58 Furthermore, an OES to whom regulation 8A(1) applies must also notify Ofcom of any changes to the information notified detailed above as soon as practicable and, in any event, within seven days beginning with the day on which the change took effect.[46]

How to notify us of a nominated person

4.59 Any person to whom the notification duties under regulations 8A(3) and 8A(4) apply must notify Ofcom in the following manner:

- send an email to nis@ofcom.org.uk;
- in the subject line of that email, state 'NIS notification – nominated person';
- state clearly in your email which above-mentioned category (or, as the case may be, categories) of deemed OES you fall into and in relation to which you are notifying a nominated person (or, as the case may be, changed details for a nominated person); for DNS Service Providers, they must specify which above-mentioned sub-category (or, as the case may be, sub-categories) is affected in that regard;
- provide your name as a designated OES – if you are a company, please also provide your company details of where you are registered overseas including full registered company name, trading name (if any), registered (head) office address, and registered company number (if any);
- provide up-to-date contact details of the nominated person (including email addresses and telephone numbers), together with (if the nominated person is a company registered in the United Kingdom) its full registered company name, trading name (if any), registered office address, and registered company number.

4.60 Any failure to comply with the notification requirements under regulation 8A may be enforced by Ofcom under regulation 17 and we may also impose penalties under regulation 18 in relation to such a failure (see Section 9 of this Guidance).

Our powers in relation to an OES and its nominated person

4.61 Regulation 8A(5) provides that we and GCHQ (the NCSC) may, for the purposes of carrying out our responsibilities under the Amended NIS Regulations, contact the nominated person instead of or in addition to the OES.

[46] Regulation 8A(4).

4.62 In that regard, we would normally expect to serve any document or notice required or authorised by the Amended NIS Regulations, including in accordance with regulation 24, on the nominated person. We may also send a copy of any such document or notice to the OES itself, where we consider it appropriate on a case-by-case basis.

4.63 Any nomination under regulation 8A(3) is also without prejudice to any legal action which we could initiate against the OES.[47]

Our administration of OES designations

4.64 We will maintain a list of all the persons who are deemed to be designated as an OES under regulation 8(1) or designated as an OES by us under regulation 8(3) for the digital infrastructure subsector.[48]

4.65 We will also review that list at regular intervals, at least biennially.[49]

4.66 We will also keep a list of all the revocations made under regulation 9.[50]

4.67 We must also send a copy of the above-mentioned lists to GCHQ (the NCSC) as the SPOC to enable it to prepare the report mentioned in regulation 4(3).[51]

[47] Regulation 8A(6).
[48] Regulations 3(3)(c) and 8(8).
[49] Regulation 8(9).
[50] Regulation 3(3)(d).
[51] Regulation 3(3)(e).

5. OES security and incident reporting duties

Introduction

5.1 In this section, we deal with two main statutory duties imposed on all OES falling within the digital infrastructure subsector, whether they are deemed to be designated as OES under regulation 8(1) or designated by us as OES under regulation 8(3). Those duties concern security measures and incident reporting. As mentioned in Section 2 of this Guidance, we have powers to issue guidance on the application of those duties. OES must also have regard to our guidance when carrying out their duties.[52]

OES security duties

What OES security duties are

5.2 Regulation 10 of the Amended NIS Regulations imposes on OES two distinct requirements in relation to the security of the network and information systems on which their essential service relies.

5.3 First, regulation 10(1) provides that "*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*".

5.4 In that regard, we note that, as required by regulation 10(3), those measures must ensure a level of security appropriate to the risk presented "*having regard to the state of the art*". Therefore, we will have regard to the state of the art of such measures in any compliance assessment carried out by us in relation to measures taken by OES.

5.5 Second, regulation 10(2) provides that "*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*".

Other relevant considerations

5.6 We have already explained in Section 1 of this Guidance that we recommend that OES have regard to the NIS national strategy when planning, implementing, monitoring or updating any technical and organisational security measures they take in order to comply with their duties under regulation 10.

5.7 We also note in Section 1 that the NCSC provides support to OES with cyber security advice and guidance, noting especially that the NCSC CAF Guidance brings together advice published by the NCSC that is relevant amongst other things to an OES when considering

[52] Regulations 10(4) and 11(12).

compliance with their duties under the Amended NIS Regulations, including under regulation 10.

OES significant impact incident reporting duties

What OES incident reporting duties are

5.8 Regulation 11(1) of the Amended NIS Regulations imposes a statutory duty on OES to notify us in writing of "*any incident which has a significant impact on the continuity of the essential service which that OES provides*" ("a NIS incident").

How OES should determine "significant impact"

5.9 In determining the significance of the impact of an incident, OES must[53] have regard to the following three factors:

- the number of users affected by the disruption of the essential service;
- the duration of the incident; and
- the geographical area affected by the NIS incident.

5.10 In doing so, OES must[54] have regard to our specific guidance in Table 1 below on thresholds at which we consider NIS incidents would have a significant impact on the continuity of the essential services falling within the digital infrastructure subsector.

Table 1 - Ofcom's incident reporting thresholds

Essential service for this subsector	Metric	Service Degradation
TLD Name Registry	Loss or significant degradation of >= 50% of aggregated name resolution capability (measured in queries per second)	1 hour
DNS Resolver Service	Loss or significant degradation of service to >= 50% of aggregated DNS Resolver capacity (measured in queries per second)	30 minutes
DNS Authoritative Hosting Service	Loss or significant degradation (e.g. serving incorrect results) of service for >=50% of registered domains	1 hour
IXP	Loss or significant degradation of connectivity to 25% of connected ASN; OR	1 hour
	Loss of >= 90% of total port capacity	

[53] Regulation 11(2).
[54] Regulation 11(12).

5.11 If the thresholds set out in Table 1 above are met in relation to an essential service for the digital infrastructure subsector, the OES in question should report the incident to us as a NIS incident having a significant impact.

5.12 We expect that OES providing the essential services referred to in Table 1 above will not adopt an unduly restrictive approach to interpreting our thresholds. Our general guidance is that, if there is any doubt as to whether (or not) a threshold is met, OES should take a cautious approach and submit an incident report to us on a fail-safe basis.

Promptness of reporting

5.13 Regulation 11(3) imposes a statutory duty on OES to report to us notifiable NIS incidents "*without undue delay and in any event no later than 72 hours after the operator is aware that a NIS incident has occurred*".

5.14 For the avoidance of doubt, the 72 hour-period for reporting a NIS incident to Ofcom starts from the time when an OES becomes aware that an incident has exceeded a NIS incident reporting threshold.

What and how OES must report NIS incidents to us

5.15 Regulation 11(3) requires that OES provide us with the following information when they report a NIS incident mentioned in regulation 11(1) (i.e. an incident having a significant impact):

- 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
- any other information that may be helpful to Ofcom.

5.16 However, the information to be provided by an OES is limited to information which may reasonably be expected to be within the knowledge of that OES at the time of incident reporting.[55]

5.17 Regulation 11(3) also requires that OES provide us with that information in such form and manner as we determine.

5.18 In that regard, it should be noted that NIS incident reports should be submitted by email to incident@ofcom.org.uk. In the subject line of that email, state 'NIS Incident – Significant Impact'. If you require a more secure method of communication, for example an e-mail address with enhanced security, this can be arranged on request.

5.19 Such NIS incident reports must contain the above-mentioned information by completing our 'NIS incident report form'[56], which must be attached with the above-mentioned email.

---

[55] Regulation 11(4).

[56] Our form is accessible here: https://www.ofcom.org.uk/__data/assets/rtf_file/0025/113749/Network-and-Information-Systems-incident-report-form.rtf

We give our guidance in Annex A2 on what information should be included by OES completing such NIS incident reports.

5.20 We request that the NIS incident report sets out as much information as is reasonably available at the time of reporting. Due to the above-mentioned deadline for reporting, it is possible that complete information will not be available at the time of the report. In such cases, we request that additional information is provided to us as soon as it becomes available to the OES. However, OES should not withhold reporting to us until more complete information is available.

OES reporting duties caused by Relevant Digital Service Provider (RDSP) incidents

What OES incident reporting duties are

5.21 Regulation 12(9) imposes a separate statutory duty on OES to notify Ofcom of certain Relevant Digital Service Provider (RDSP) incidents affecting the essential services provided by OES. It provides that: "*If an OES is reliant on a RDSP to provide an essential service, the operator must notify the designated competent authority for the OES in writing in relation to it about any significant impact on the continuity of the service it provides caused by an incident affecting the RDSP without undue delay.*"

5.22 In that regard, it should be noted that a RDSP is a reference to a person who provides a digital service in the United Kingdom and satisfies the following conditions:[57]

- the head office for that provider is in the United Kingdom or that provider has nominated a representative who is established in the United Kingdom;
- the provider is not a micro or small enterprise as defined in Commission Recommendation 2003/361/EC.

5.23 The concept of "digital service" is defined as a service within the meaning of point (b) of Article 1(1) of Directive 2015/1535 which is any of the following kinds:

- online marketplace;
- online search engine;
- cloud computing service.

How OES should determine "significant impact"

5.24 Unlike regulation 11(2), regulation 12 does not specify what factors an OES must have regard to in determining the significance of the impact of an incident caused by the RDSP.

5.25 We consider, however, that OES should have regard to the factors specified in regulation 11(2) also when they consider incidents falling under regulation 12(9).

[57] Regulation 1(3)(e).

Promptness of reporting

5.26 As already noted above, regulation 12(9) imposes a statutory duty on OES to report to us notifiable incidents falling under regulation 12(9) "*without undue delay*".

What and how OES must report these incidents to us

5.27 Unlike regulation 11(3), regulation 12 does not specify what information must be included in a notification falling under regulation 12(9).

5.28 We consider, however, that OES should report to Ofcom similar information to that required by regulation 11(3), as explained above. Our main guiding principle is that an OES subject to the reporting duty in regulation 12(9) should obtain as much information as is reasonably possible from the affected RDSP before sending an incident report to Ofcom.

5.29 Accordingly, we request that affected OES complete our above-mentioned 'NIS incident report form'. That form must include the information set out in paragraph 5.15 above and also include the RDSP related information in that incident report description, which should as a minimum include:

- the RDSP name and the essential services that were affected;
- the time the RDSP incident occurred;
- the duration of the RDSP incident;
- information concerning the nature and impact of the RDSP incident;
- information concerning any, or any likely, cross-border impact of the RDSP incident; and
- any other information that may be helpful to Ofcom.

We give guidance in Annex A2 on the information which OES should include when completing such NIS incident reports, including informing other authorities if necessary.

5.30 Such incident reports containing the above-mentioned form and information should be submitted by email to incident@ofcom.org.uk. In the subject line of that email, state 'NIS Incident – Significant Impact (RDSP caused)'. If you require a more secure method of communication, for example an e-mail address with enhanced security, this can be arranged on request.

Voluntary incident reporting

5.31 We request that OES report to us incidents that may not have exceeded the incident thresholds discussed above, but which had the possibility to exceed a threshold. We also request such voluntary reports for incidents caused by RDSPs even if they do not have significant impact but which may have had the possibility of having such impact. For example, those incidents where, without corrective action, a reporting threshold would likely have been exceeded. This is because such voluntary incident reports will assist us in identifying thematic issues across the digital infrastructure subsector.

5.32 We welcome that such voluntary incidents reports are made to Ofcom in the same manner and form as set out above for mandatory NIS incidents having a significant impact. In doing so, please state in the subject line of the email 'NIS Incident – Voluntary Report'.

5.33 We also request that OES complete our above-mentioned 'NIS incident report form' for such voluntary incident reports, making it clear in that form that the report is provided voluntarily.

5.34 Ofcom will not share any voluntarily reported incidents with any third-party, such as the NCSC.

Our responsibilities for reported NIS incidents

5.35 After we receive a NIS incident report under regulation 11(1) from an OES, we are required to assess what further action (if any) is required in respect of that incident and to share the NIS incident information with the NCSC as soon as reasonably practicable.[58]

5.36 After we receive a NIS incident report, we or the NCSC may also inform:

- the OES who reported the NIS incident to us about any relevant information that relates to the NIS incident, including how it has been followed up, in order to assist that OES to deal with that incident more effectively or prevent a future incident; and
- the public about the NIS incident, as soon as reasonably practicable, if we or the NCSC is of the view that public awareness is necessary in order to handle that incident or prevent a future incident.

5.37 Before we or the NCSC informs the public about a NIS incident, we or the NCSC must consult each other and the OES who reported the NIS incident to us.

5.38 We are also required to provide an annual report to the NCSC identifying the number and nature of NIS incidents reported to us. We must submit that annual report on or before 1 July every year.

OES potential wider reporting duties

5.39 We note that our role under the Amended NIS Regulations does not include incident response.

5.40 Any NIS incident reporting to us should not be treated as a substitute for OES reporting to other regulatory authorities, agencies or bodies as required.

[58] Regulation 11(5).

6. Our information sharing powers

What our information sharing powers are

6.1 Regulation 6 of the Amended NIS Regulations gives Ofcom powers to share information with other NIS enforcement authorities[59], relevant law-enforcement authorities[60], the CSIRT, and public authorities in the EU.

6.2 We may only share information with the above-mentioned authorities (including the CSIRT) if two preconditions set out in regulation 6(1) are satisfied.

Purposes for which we may share information

6.3 The first precondition is that, as a general rule, our information sharing must be necessary for one or more of the following purposes:

- the purposes of the Amended NIS Regulations or of facilitating the performance of any functions of a NIS enforcement authority under or by virtue of the Amended NIS Regulations or any other enactment;
- national security purposes; or
- purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution.

6.4 In relation to that first precondition, we say as a "general rule" because regulation 6(1A) contains an exception, namely that information shared under regulation 6(1) may not be further shared by the person with whom it is shared under regulation 6(1) for any purpose other than a purpose mentioned in regulation 6(1) "*unless otherwise agreed by the NIS enforcement authority*" (i.e. Ofcom in this case). We therefore have the power to agree for the information to be shared for other purposes. We will consider the application of that exception on a case-by-case basis, should it arise.

Limited extent of our information sharing

6.5 The second precondition is that our information sharing must be limited to information which is relevant and proportionate to the purpose of the information sharing.

6.6 What information is relevant and proportionate to share with another authority will depend on the circumstances in each case. Before sharing information with another authority, we will seek enough information from that authority to satisfy ourselves that this second precondition is satisfied.

[59] Regulation 1(3)(f) clarifies that a reference in the Amended NIS Regulations to "NIS enforcement authorities" is a reference to the competent authorities designated under regulation 3(1) and the Information Commissioner.
[60] See Section 1 of this Guidance for the meaning of "relevant law-enforcement authorities".

What kind of information may be shared

6.7 Regulation 6 does not prescribe that our information sharing powers are limited to (for example) information with respect to a particular business which we may obtain in exercise of our powers to serve information notices (see Section 7 of this Guidance).

6.8 Therefore, the kind of information we may share pursuant to our information sharing powers is wide-ranging and it may include also any informal information that we receive and hold from stakeholders from time to time, additionally to any information we receive pursuant to (for example) our information gathering powers.

6.9 We may also share other kinds of information that we receive and hold in exercising our other functions under the Amended NIS Regulations.

6.10 For example, OES are required to report to us significant incidents under regulation 11, which may contain information that we may be asked to share with other enforcement authorities. However, we have already explained in Section 5 of this Guidance that we will not share any voluntarily reported incidents with any third-party, such as the NCSC.

6.11 Another example is information we obtain when exercising our power of inspection under regulation 16.

6.12 The information we share pursuant to our information sharing powers may also include confidential information or otherwise commercially sensitive information. However, regulation 6(2) clarifies that, when we share information with a public authority in the EU, we are not required to share confidential information, or information which may prejudice the security or commercial interests of an OES.

Our information sharing will be undisclosed

6.13 We will normally not contact a person whose information we are sharing with another authority under regulation 6.

6.14 We consider that there are reasons why it would be inappropriate for us to contact the person who has provided us with the information about our intended information sharing.

6.15 For example, the purposes for which information may be shared with other enforcement authorities under regulation 6 include circumstances where they are taking enforcement action, or measures to prevent or detect crime. If we were to contact the person who has provided us with the information, it could alert that person to what those other enforcement authorities are doing and it could therefore risk jeopardising the functions they are carrying out.

7. Our information gathering powers

What our powers are

Purposes for which we may obtain information

7.1 Regulation 15 of the Amended NIS Regulations gives Ofcom powers to require the provision of information for the purposes specified in regulation 15.

7.2 We may[61] require information from "any person" (including, but not limited to, from someone who we suspect may fall within regulation 8(1) as a deemed OES) to assess whether a person should be an OES by establishing whether:

- a threshold requirement described in Schedule 2 to the Amended NIS Regulations is met; or
- the conditions mentioned in regulation 8(3) are met.

7.3 We may[62] also require information from "an OES" (but not from any other person) to:

- assess the security of the OES's network and information systems;
- establish whether there have been any events that we have reasonable grounds to believe have had, or could have, an adverse effect on the security of network and information systems and the nature and impact of those events;
- identify any failure of the OES to comply with any duty set out in the Amended NIS Regulations;
- assess the implementation of the OES's security policies, including from the results of any inspection conducted under regulation 16 and any underlying evidence in relation to such an inspection.

7.4 We can only gather the information if it is reasonably required for one or more of above-mentioned purposes. However, in carrying out our functions under the Amended NIS Regulations, Ofcom normally needs reliable evidence upon which we can base our decisions which therefore often necessitates our need to gather information.

7.5 We gather such information by serving an "information notice", the contents and service of which we detail below.

Our use of the obtained information for a different purpose

7.6 We will always explain in our information notices the purpose(s) for which we are requiring the specified information.

7.7 Where Ofcom has obtained information for a specified purpose and then wishes to use that information for a different purpose, we will contact the person who provided the information, providing our reasons as to why we need to use the information for a

[61] Regulation 15(1).
[62] Regulation 15(2).

different purpose. In so doing, we will give that person a short period to let us know if it has any concerns about our intention to use the information for another purpose.

7.8 Unless the circumstances require otherwise, we would normally not require that person to resubmit the information it has already provided to Ofcom. However, if relevant, the person should take the opportunity to inform Ofcom of any changes that might affect the accuracy or completeness of the previously submitted information in commenting on our intended use of the information for a different purpose.

7.9 If the person objects to our use of the information for another purpose, we will carefully consider the person's reasons for such objection. If we nonetheless decide that it is appropriate and necessary to use the information for the other purpose, we will let the person know that we intend to do so.

7.10 However, as already explained in Section 6 of this Guidance, we will normally not contact a person who has provided us with information in response to our information notice, where we intend to share information with other enforcement authorities under regulation 6 of the Amended NIS Regulations. In such cases, we would carefully consider whether the information sharing is necessary for the purposes mentioned in regulation 6. If the information sharing is necessary, we will limit our sharing to information which is relevant and proportionate to the purpose of the information sharing.

Statutory duty to comply with information notices

7.11 Regulation 15(5A) imposes a statutory duty in that a person upon whom an information notice has been served under regulation 15 must comply with the requirements of the notice.

7.12 Any failure to comply with an information notice issued under regulation 15 may be enforced by Ofcom under regulation 17 and we may also impose penalties under regulation 18 in relation to such a failure (see Section 9 of this Guidance).

How we will gather information

Contents of our information notices

7.13 Regulation 15(5) requires that an information notice must:

- describe the information that is required by Ofcom;
- provide our reasons for requesting such information;
- specify the form and manner in which the requested information is to be provided; and
- specify the time period within which the information must be provided.

7.14 Where timescales allow and it is appropriate to do so, Ofcom will send a draft of an information notice to the person holding the relevant information for any comments in relation to our intended content of, or deadline for responding to, the notice.

7.15 For example, we may decide it is appropriate to send our information notices in draft form for comments where the information being requested is complex, it is unclear to Ofcom

how best to ask for specific information to ensure that we get the information needed or we would like to understand (ahead of serving our final notice) whether the information is held in the format requested. In contrast, we may decide that it is appropriate to send our information notices in final form only (i.e. without inviting any comments) where (for example) the information we are seeking is less complex or we need to receive it urgently.

7.16 Where we invite comments on our information notices, the amount of time we give to make such comments will depend on the circumstances of each case.

7.17 Following our receipt of any such comments, we will carefully consider them before either confirming or amending the notice. Then, we would normally proceed to serve our information notice on the person without a further round of comments regarding the content or the deadline.

Our service of information notices

7.18 Regulation 24 of the Amended NIS Regulations requires that any document or notice required or authorised by these Regulations (including information notices) to be served on a person may be served by:

- delivering it to that person in person;
- leaving it at the person's proper address; or
- sending it by post or electronic means to that person's proper address.

7.19 For those purposes, "proper address" means:[63]

> "*(a) in the case of a body corporate or its director—*
>
> *(i) the registered or principal office of that body; or*
>
> *(ii) the email address of the secretary or clerk of that body;*
>
> *(b) in the case of a partnership, a partner or person having control or management of the partnership business—*
>
> *(i) the principal office of the partnership; or*
>
> *(ii) the email address of a partner or a person having that control or management;*
>
> *(c) in any other case, a person's last known address, which includes an email address.*"

7.20 If a person has specified an address in the United Kingdom (other than that person's proper address) at which that person or someone on that person's behalf will accept service, that address must also be treated as that person's proper address.[64]

7.21 If an OES has nominated a person to act on its behalf in the United Kingdom (see Section 4 of this Guidance), we would serve our information notice on that nominated person.

[63] Regulation 24(5).
[64] Regulation 24(4).

7.22 The exception[65] to the above-mentioned means of serving our information notices is where we gather information to assess whether a person should be an OES under regulation 15(1) of the Amended NIS Regulations. In such cases, we may serve our information notice by publishing it in such manner as we consider appropriate in order to bring it to the attention of any persons who are described in the notice as the persons from whom the information is required; and take the form of a general request for a certain category of persons to provide the information that is specified in the notice. The reason for this exception is that we may not know the identity of the person(s) holding the relevant information that we require for the purpose of assessing whether a person should be an OES.

How to respond to our information notices

Our Information Registry

7.23 As an evidence-based regulator, Ofcom regularly requests information from stakeholders to inform all aspects of our work. We have statutory powers for such information gathering in order to ensure we receive accurate and complete information from companies in a timely manner.

7.24 We have a dedicated team, our Information Registry, that manages information requests. The Information Registry offers an end-to end process for making information requests and collating responses. It also acts as a central contact point for stakeholders on information gathering matters. The Information Registry can be contacted at information.registry@ofcom.org.uk. It also logs and tracks all formal information requests, whilst monitoring stakeholder compliance in responding.

Manner and form of responding

7.25 Our information notices will specify how addressees of our notices should respond. We normally ask for the information to be provided electronically by email (the address details of which will be set out in our notices) or by our preferred method of uploading it to Ofcom's secure server using a Managed File Transfer (MFT) service.

7.26 To use the MFT option, we request in our information notices that the addressee should email named individuals in our notice some working days before the deadline, and provide the name and email address of the addressee's nominated contact who will upload the data. This is because we need some time to set up an account. An information sheet about the MFT service will be enclosed in our information notices.

Confidentiality

7.27 We will ask in our information notices that addressees set out clearly in a separate annex marked "confidential information" any document or information which they consider to be confidential and supply a written explanation as to why it should be treated as such.

[65] Regulation 15(6).

7.28 Ofcom will take into consideration any representations addressees make when determining which information it considers to be confidential. However, blanket claims of confidentiality are unhelpful and are not likely to be accepted. Ultimately, it is for Ofcom to determine what is, and is not, confidential.

Personal data

7.29 We will process any personal data contained in our information notices or provided in response to them in accordance with Ofcom's General Privacy Statement.

7.30 We consider that any personal data addressees process in responding to our information notices will be processed by them on their own account, as a data controller, rather than as a processor of that data for Ofcom. They will be responsible for complying with their own obligations under relevant data protection legislation. They may also wish to inform any employees whose personal data they will be providing in response to our notices that their personal data is being provided to Ofcom and provide a link to Ofcom's General Privacy Statement.

Withdrawal of information notices

7.31 In the exceptional circumstances that we should no longer require the information specified in our information notices, we will withdraw an information notice by written notice to the person on whom it was served.[66]

[66] Regulation 15(7).

8. Our powers of inspection

What our powers are

Our powers to conduct an inspection

8.1 Regulation 16(1) of the Amended NIS Regulations gives Ofcom powers to conduct ourselves, or appoint another person (third party) to conduct on our behalf, all or any part of an inspection of an OES. We may also direct an OES to appoint a person approved by us to carry out all or any part of an inspection on our behalf.

8.2 Any person conducting all or any part of an inspection in accordance with regulation 16(1) is called an "inspector".[67]

8.3 Where we appoint another person (third party) to conduct all or any part of an inspection on our behalf, we may do so on such terms and in such a manner as we consider appropriate.[68]

Meaning (and purposes) of an "inspection"

8.4 For the purposes of regulation 16, an "inspection" means[69] any activity carried out (including any steps mentioned in regulation 16(5)) for the purpose of:

- verifying compliance with the requirements of the Amended NIS Regulations; or
- assessing or gathering evidence of potential or alleged failures to comply with the requirements of the Amended NIS Regulations,
- including any necessary follow-up activity for either purpose.

Powers of an inspector

8.5 Regulation 16(5) provides that an inspector may:

[67] Regulation 16(9)(c).
[68] Regulation 16(4).
[69] Regulation 16(9)(b).

"*(a) at any reasonable time enter the premises of an OES or RDSP (except any premises used wholly or mainly as a private dwelling) if the inspector has reasonable grounds to believe that entry to those premises may be necessary or helpful for the purpose of the inspection;*

(b) require an OES or RDSP to leave undisturbed and not to dispose of, render inaccessible or alter in any way any material, document, information, in whatever form and wherever it is held (including where it is held remotely), or equipment which is, or which the inspector considers to be, relevant for such period as is, or as the inspector considers to be, necessary for the purposes of the inspection;

(c) require an OES or RDSP to produce and provide the inspector with access, for the purposes of the inspection, to any such material, document, information or equipment which is, or which the inspector considers to be, relevant to the inspection, either immediately or within such period as the inspector may specify;

(d) examine, print, copy or remove any document or information, and examine or remove any material or equipment (including for the purposes of printing or copying any document or information) which is, or which the inspector considers to be, relevant for such period as is, or as the inspector considers to be, necessary for the purposes of the inspection;

(e) take a statement or statements from any person;

(f) conduct, or direct the OES or RDSP to conduct, tests;[70]

(g) take any other action that the inspector considers appropriate and reasonably required for the purposes of the inspection."

Duties of an inspector

8.6 Regulation 16(6) requires that an inspector:

- produces proof of their identity if requested by any person present at the premises; and
- takes appropriate and proportionate measures to ensure that any material, document, information or equipment removed in accordance with regulation 16(5)(d) is kept secure from unauthorised access, interference and physical damage.

8.7 In addition, before exercising any power under regulation 16(5)(b) to (d) or (g), the inspector:[71]

- must take such measures as appear to the inspector appropriate and proportionate to ensure that the ability of the OES to comply with any duty set out in the Amended NIS Regulations will not be affected; and

[70] Regulation 16(9)(a) explains that a "test" is a reference to any process which is: (i) employed to verify assertions about the security of a network or information system; and (ii) based on interacting with that system, including components of that system, and includes the exercising of any relevant security or resilience management process.
[71] Regulation 16(7).

- may consult such persons as appear to the inspector appropriate for the purpose of ascertaining the risks, if any, there may be in doing anything which the inspector proposes to do under that power.

8.8 Furthermore, where under regulation 16(5)(d), an inspector removes any document, material or equipment, the inspector must provide, to the extent practicable, a notice giving:

- sufficient particulars of that document, material or equipment for it to be identifiable; and
- details of any procedures in relation to the handling or return of the document, material or equipment.

Duties of an OES in relation to an inspection

8.9 Regulation 16(3) imposes the following duties on an OES for the purposes of any inspection:

- OES must pay the reasonable costs of the inspection if so required by Ofcom;
- OES must co-operate with the inspector;
- OES must provide the inspector with access to the premises in accordance with regulation 16(5)(a);
- OES must allow the inspector to examine, print, copy or remove any document or information, and examine or remove any material or equipment, in accordance with regulation 16(5)(d);
- OES must allow the inspector access to any person from whom the inspector seeks relevant information for the purposes of the inspection;
- OES must not intentionally obstruct an inspector performing their functions under the Amended NIS Regulations; and
- OES must comply with any request made by, or requirement of, an inspector performing their functions under the Amended NIS Regulations.

8.10 Any failure to comply with a direction given under regulation 16(1)(c) or the requirements stipulated in regulation 16(3) may be enforced by Ofcom under regulation 17 and we may also impose penalties under regulation 18 in relation to such a failure (see Section 9 of this Guidance).

9. Our enforcement action and penalties

What this section covers

9.1 In this section, we set out how we will approach enforcement action in cases relating to relevant failures to comply with relevant requirements of the Amended NIS Regulations, together with our imposition of any penalties on OES.

9.2 In general, we normally expect that our approach to enforcement of the Amended NIS Regulations would be broadly in line with the approach we take in cases relating to electronic communications networks and services, postal services and some cases relating to breaches of wireless telegraphy licences, as set out in our Enforcement Guidelines for regulatory investigations published on 28 June 2017 (the "Enforcement Guidelines").[72]

9.3 However, some process steps, powers and associated process requirements set out in the Amended NIS Regulations differ in some respects from our powers and required processes that apply for our regulatory investigations covered by the Enforcement Guidelines. We therefore reserve our position to follow different approaches permitted under the Amended NIS Regulations in specific cases, where we consider it is appropriate to do so.

9.4 We explain in this section by reference to the Enforcement Guidelines how they should be generally read in relation to any enforcement action we might take under the Amended NIS Regulations. We also explain below how our Penalty Guidelines[73], as published on 14 September 2017 under section 392 of the Communications Act 2003, are relevant also in relation to any penalties we may impose on OES under the Amended NIS Regulations.

9.5 We recommend that stakeholders read our guidance below in parallel with our Enforcement Guidelines and Penalty Guidelines for a fuller understanding of our intended approach under the Amended NIS Regulations.

Our objectives

Objectives in our Enforcement Guidelines

9.6 Section 1 of the Enforcement Guidelines[74] explains that we take enforcement action in respect of non-compliance with statutory or regulatory requirements in order to prevent harm to consumers and competition, and to remedy this where we can. We may also impose a penalty to deter non-compliance. We also explain in that Section 1 that we seek to ensure that enforcement action is conducted in a fair, transparent, efficient and timely way. Those objectives will apply also in relation to any enforcement action we take (including any penalties we impose) under the Amended NIS Regulations.

---

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

[73] https://www.ofcom.org.uk/about-ofcom/policies-and-guidelines/penalty-guidelines

[74] See paragraphs 1.6 and 1.7 of the Enforcement Guidelines.

9.7 However, some additional considerations arise under the Amended NIS Regulations that we must take into account in taking any enforcement action, which we detail below.

The NIS national strategy

9.8 As explained in Section 1 of this Guidance, regulation 3(6) of the Amended NIS Regulations provides that we must have regard to the NIS national strategy when carrying out our duties under the NIS Regulations.

9.9 In that regard, we note that regulation 2(2) provides that the strategic objectives and priorities set out in the NIS national strategy must be aimed at achieving and maintaining a high level of security of network and information systems in sectors, such as the digital infrastructure subsector for which Ofcom is responsible. One of the matters that the NIS national strategy must address is the regulatory measures and enforcement framework to secure the objectives and priorities of the strategy.[75]

General considerations for any enforcement action

9.10 Regulation 23 of the Amended NIS Regulations requires that, before we take any action under regulations 17(1)[76], 18(3A)[77] or A20[78], we must consider whether it is reasonable and proportionate, on the facts and circumstances of the case, to take action in relation to the contravention.

9.11 In particular, we must have regard to the following matters:

- any representations made by the OES about the contravention and the reasons for it, if any;
- any steps taken by the OES to comply with the requirements set out in the Amended NIS Regulations;
- any steps taken by the OES to rectify the contravention;
- whether the OES had sufficient time to comply with the requirements set out in the Amended NIS Regulations; and
- whether the contravention is also liable to enforcement under another enactment.

9.12 Those general considerations are consistent with considerations that we are already required to have regard to in securing our general duties under section 3 of the Communications Act 2003 in carrying out all of our functions. We list those general duties in Section 3 of this Guidance, and they are further detailed in Section 2 of the Enforcement Guidelines.

[75] Regulation 2(5)(a).
[76] The service of an enforcement notice on an OES.
[77] The service of a penalty notice with a final penalty decision on an OES.
[78] Enforcement by civil proceedings.

Why and how Ofcom opens cases

Contents of Section 2 of the Enforcement Guidelines

9.13 Section 2 of the Enforcement Guidelines explains the following matters:

- why we open cases;
- sources of information;
- complaints and whistleblowing;
- initial assessment;
- resolution through means other than formal action; and
- next steps following our decision on whether to open an investigation.

9.14 Those matters will be generally relevant also in our consideration of taking any enforcement action under the Amended NIS Regulations.

Our consideration of typical factors in deciding to open a case

9.15 In that Section 2, we detail (and give examples of) three particular factors that we will generally consider in deciding whether we should open investigations, namely:

- the risk of harm arising from/seriousness of the alleged conduct;
- the strategic significance of addressing the alleged conduct and whether alternative proceedings are likely to achieve the same ends; and
- the resource implications of our conducting an investigation.

9.16 We also mention in that Section 2 that, where appropriate, we will also consider other factors as well. We have already mentioned (in detailing our objectives above) that we will have regard to some additional considerations that arise under the Amended NIS Regulations, such as the NIS national strategy and the general considerations set out in regulation 23 of the Amended NIS Regulations.

9.17 We also have duties under regulation 3(3) of the Amended NIS Regulations to:

- consult and co-operate with the Information Commissioner when addressing incidents that result in breaches of personal data; and
- consult and co-operate with relevant law-enforcement authorities; other competent authorities in the United Kingdom; the SPOC that is designated under regulation 4; and the CSIRT that is designated under regulation 5.

9.18 We may therefore also consider those consultation and co-operation duties in deciding on whether we consider it is appropriate to open an investigation under the Amended NIS Regulations.

Our sources of information

9.19 One of the sources of information (which could trigger our investigation) detailed in Section 2 of the Enforcement Guidelines is information provided to us by other bodies.

9.20 In that regard, it is relevant to note that the CSIRT must co-operate with NIS enforcement authorities to enable the enforcement authorities to fulfil their obligations under the Amended NIS Regulations. In addition, under regulation 6, the NIS enforcement authorities may share information with each other, relevant law-enforcement authorities, and the CSIRT, if that information sharing is necessary for (among other things) taking enforcement action under the Amended NIS Regulations.

Complaints and whistleblowing

9.21 We also set out in Section 2 of the Enforcement Guidelines our guidance for stakeholders who wish to make a complaint or whistleblowing in the communications sector. That guidance is relevant also to our stakeholders in relation to our role under the Amended NIS Regulations.

Our initial assessment

9.22 Our process to carry out an initial assessment is detailed in paragraphs 2.12 to 2.21 of the Enforcement Guidelines and we expect that it would normally be followed also for any potential investigation under the Amended NIS Regulations.

9.23 Likewise, our normal process to resolve an issue without the need for formal investigation detailed in Section 2 of the Enforcement Guidelines is also relevant to any enforcement related activity we may carry out under the Amended NIS Regulations.

9.24 We would also normally follow the next steps of Ofcom's decision on whether to open an investigation explained in paragraphs 2.27 to 2.33 of the Enforcement Guidelines.

Investigating

Contents of Section 3 of the Enforcement Guidelines

9.25 Section 3 of the Enforcement Guidelines sets out how we are likely to conduct an investigation, including guidance on our likely engagement and contact with the subject of the investigation, complainants and third parties, and how we will gather and publish information and deal with confidential information.

9.26 In broad outline, we expect that the initial process described in that Section 3 will be the same (or similar) for investigations under the Amended NIS Regulations.

Our information gathering

9.27 In paragraph 3.16 of the Enforcement Guidelines, we set out where our statutory powers to gather information come from. That paragraph should be read as including references to

both regulation 15 (information notices)[79] and regulation 16 (power of inspection)[80] of the Amended NIS Regulations.

Our approach to confidentiality

9.28 Our approach to dealing with confidentiality detailed in paragraphs 3.19 to 3.22 of the Enforcement Guidelines is broadly relevant also to our investigations under the Amended NIS Regulations. However, there are some important differences compared to our regulatory investigations subject to the Enforcement Guidelines.

9.29 We have already mentioned above that we may, under regulation 6 of the Amended NIS Regulations, share information with other NIS enforcement authorities, relevant law-enforcement authorities and the CSIRT, if that information sharing is necessary for (among other things) taking enforcement action. In doing so, our information sharing must be limited to information which is relevant and proportionate to the purpose of the information sharing. Such disclosure will depend on the facts and circumstances in each case and we will decide on the best means of dealing with any confidential information on a case-by-case basis.

9.30 Another difference relates to statutory general restrictions on our disclosure (such as under section 393 of the Communications Act 2003) for regulatory investigations subject to the Enforcement Guidelines. There are no corresponding general restrictions[81] on our disclosure of information under the Amended NIS Regulations. However, we intend to take steps, so far as is possible, to protect the legitimate interests of stakeholders in relation to confidential and commercially sensitive information. In particular, we would only seek to disclose such information to the extent we consider it necessary for the purpose of taking any enforcement action under the Amended NIS Regulations.

Other matters in Section 3 of the Enforcement Guidelines

9.31 Section 3 of the Enforcement Guidelines also explains the following matters (which will be relevant also to our investigations under the Amended NIS Regulations):

- publicising cases;
- involvement of third parties; and
- how to raise concerns with Ofcom.

[79] See further in Section 7 of this Guidance for our information gathering powers under the Amended NIS Regulations.
[80] See further in Section 8 of this Guidance for our powers of inspection under the Amended NIS Regulations.
[81] Section 393 of the Communications Act 2003 only applies when we exercise powers conferred by the Communications Act 2003, the Broadcasting Act 1990 and the Broadcasting Act 1996.

Outcomes of regulatory investigations and the decision-making process

Four different broad possible outcomes

9.32 Section 4 of the Enforcement Guidelines covers how we decide on the outcome of a regulatory investigation and who will make key decisions during an investigation.

9.33 We explain in paragraphs 4.3 and 4.4 of the Enforcement Guidelines that there are typically four different broad outcomes of regulatory investigations, namely:

- we may decide that there are grounds for action;
- we may decide that there is insufficient evidence of a contravention, and close the case on that basis (potentially subject to a period of compliance monitoring);
- we may decide to close a case without having taken a final decision on the merits of a case; and
- in some cases, we may be able to reach a settlement with the subject of an investigation as a way of resolving a case, in circumstances where we have grounds to reach an enforcement decision (the process for settlement is detailed in Section 5 of the Enforcement Guidelines).

9.34 Those possible broad outcomes apply also for our investigations under the Amended NIS Regulations.

9.35 However, where we decide that there are grounds for action, Section 4 of the Enforcement Guidelines is based on a typical process for issuing provisional breach notifications as prescribed by statute in relation to many of our enforcement functions, such as under the Communications Act 2003. That typical process has some equivalent aspects under the Amended NIS Regulations, but with some important differences.

9.36 We explain below the processes set out in the Amended NIS Regulations for serving enforcement and penalty notices, before setting out the approach we would normally expect to take in the majority of investigations, where possible, under the Amended NIS Regulations. We will also explain how Section 4 of the Enforcement Guidelines should be read in light of those clarifications.

Forms of enforcement action under the Amended NIS Regulations

9.37 Enforcement action under the Amended NIS Regulations can take two forms:

- enforcement notices under regulation 17; and/or
- penalty notices under regulation 18.

9.38 Those forms apply separately from our powers under regulation 16 to conduct an inspection, which powers we discuss in Section 8 of this Guidance.

Enforcement notices under regulation 17

Our notices of our intention to serve enforcement notices

9.39 The main focus (and its starting point) in regulation 17 is on the service of enforcement notices (which we discuss below). However, regulation 17(2A) provides that, before we serve an enforcement notice under regulation 17(1), we must inform the OES, in such form and manner as we consider appropriate having regard to the facts and circumstances of the case, of the alleged failure and how and by when representations may be made in relation to the alleged failure and any related matters. In doing so, regulation 17(2B) provides that we may also provide our notice of our intention to serve an enforcement notice.

9.40 After we have informed the OES in accordance with regulation 17(2A), and following our consideration of any representations that the OES has made to us, regulation 17(2C) provides that we may serve our enforcement notice under regulation 17(1) on the OES within a reasonable time, irrespective of whether we have provided any notice of our intention to serve an enforcement notice in accordance with regulation 17(2B), having regard to the facts and circumstances of the case.

9.41 In other words, we have a choice as to whether we inform an OES in accordance with regulation 17(2A) or whether we do so by providing an OES with a notice of our intention to serve an enforcement notice. We would normally expect to serve an OES with a notice of our intention to serve an enforcement notice to inform the OES of the matters referred to in regulation 17(2A), although we note that in some cases the circumstances may require us to do otherwise. We further discuss below our expected normal approach to serving our notices where there are grounds for action.

Our enforcement notices

9.42 Regulation 17(1) gives us the power to serve an enforcement notice[82] on OES falling within the digital infrastructure subsector, if we have reasonable grounds to believe that an OES has failed to comply with any of the various duties and requirements listed in that regulation, namely:

- failure to notify us under regulation 8(2);
- failure to comply with the requirements stipulated in regulation 8A;
- failure to fulfil the security duties under regulation 10(1) and (2);
- failure to notify us of a NIS incident under regulation 11(1);
- failure to comply with the notification requirements stipulated in regulation 11(3);
- failure to notify us of an incident as required by regulation 12(9);
- failure to comply with our information notices issued under regulation 15; or

[82] Pursuant to regulation 17(3), an "enforcement notice" must be in writing and must specify the reasons for serving the notice; the alleged failure which is the subject of the notice; and what steps, if any, must be taken to rectify the alleged failure and the time period during which such steps must be taken.

- failure to comply with our directions given under regulation 16(1)(c) or the requirements stipulated in regulation 16(3).

9.43 Regulation 17(3A) imposes a statutory duty on an OES upon whom we have served an enforcement notice under regulation 17(1) to comply with the requirements (if any) of the notice, regardless of whether the OES has paid any penalty imposed on it under regulation 18.

9.44 Our enforcement notices amount, in their effect, to enforcement decisions. This is because of the above-mentioned duty in regulation 17(3A), which may be enforced by us under regulation A20 of the Amended NIS Regulations. In particular, we have the power to commence civil proceedings, for example, for an injunction to enforce that duty, if we have reasonable grounds to believe that an OES has failed to comply with the requirements of an enforcement notice.

Our decisions to take no further action

9.45 We also note that regulation 17(4) provides that, if we are satisfied that no further action is required having considered any representations submitted by an OES in accordance with regulation 17(2A) or any steps taken by the OES to rectify the alleged failure, we must inform the OES in writing as soon as reasonably practicable.

9.46 The OES may also request our reasons for a decision to take no further action within 28 days of being informed of that decision.[83] Upon receipt of such a request, we must provide written reasons for a decision under regulation 17(4) within a reasonable time and in any event no later than 28 days.[84]

Penalty notices under regulation 18

Our notices of our intention to impose penalties

9.47 Regulation 18(1) gives us the power to serve a notice of intention to impose a penalty[85] on an OES, if we have reasonable grounds to believe that the OES has failed to comply with a duty referred to in regulation 17(1) or the duty set out in regulation 17(3A) and we consider that a penalty is warranted having regard to the facts and circumstances of the case.

Our penalty notices with our final penalty decisions

9.48 After considering any representations submitted by an OES in accordance with the requirements of our notice of intention to impose a penalty, regulation 18(3A) gives us the

[83] Regulation 17(5).
[84] Regulation 17(6).
[85] Pursuant to regulation 18(3), a "notice of intention to impose a penalty" must be in writing and must specify the reasons for imposing a penalty; the sum that is intended to be imposed as a penalty and how it is to be paid; the date on which the notice of intention to impose a penalty is given; the period within which a penalty will be required to be paid if a penalty notice is served; that the payment of a penalty under a penalty notice (if any) is without prejudice to the requirements of any enforcement notice (if any); and how and when representations may be made about the content of the notice of intention to impose a penalty and any related matters.

power to serve a penalty notice[86] on the OES with a final penalty decision, if we are satisfied that a penalty is warranted having regard to the facts and circumstances of the case.

9.49 Regulation 18(3C) also provides that we may serve a notice of intention to impose a penalty or a penalty notice irrespective of whether we have served or are contemporaneously serving an enforcement notice on the OES under regulation 17(1). In other words, we have a choice as to whether we decide to serve a separate enforcement notice on the OES under regulation 17(1). We discuss below our expected normal approach to serving our notices where there are grounds for action.

9.50 Regulation 18(3E) imposes a statutory duty on the OES to comply with any requirement imposed by a penalty notice. Regulation 20 deals with the enforcement of penalty notices.

9.51 We may also withdraw a penalty notice by informing the person upon whom it was served in writing.[87]

Maximum penalty amounts

9.52 The maximum levels of penalty under a penalty notice is covered by regulation 18(5). It provides that the sum of any penalty imposed must be an amount that Ofcom determines is appropriate and proportionate to the failure in respect of which it is imposed, and is in accordance with regulation 18(6), namely:

> "*(6) The amount must—*
>
> *(a) not exceed £1,000,000 for any contravention which the NIS enforcement authority determines was not a material contravention;*
>
> *(c) not exceed £8,500,000 for a material contravention which the NIS enforcement authority determines does not meet the criteria set out in sub-paragraph (d); and*
>
> *(d) not exceed £17,000,000 for a material contravention which the NIS enforcement authority determines has or could have created a significant risk to, or significant impact on, or in relation to, the service provision by the OES or RDSP.*"

9.53 A "material contravention" means[88]:

[86] Pursuant to regulation 18(3D), a "penalty notice" must be in writing and must include reasons for the final penalty decision; require the OES to pay the penalty specified in the notice of intention to impose a penalty or such penalty as Ofcom considers appropriate in the light of any representations made by, and any steps taken by, the OES to rectify the failure or to do one or more of the things required by an enforcement notice under regulation 17(3); specify the period within which the penalty must be paid ("the payment period") and the date on which the payment period is to commence; provide details of the appeal process under regulation 19A; and specify the consequences of failing to make payment within the payment period.
[87] Regulation 18(4).
[88] Regulation 18(7)(a).

- a failure to take, or adequately take, one or more of the steps required under an enforcement notice within the period specified in that notice to rectify a failure described in one or more of sub-paragraphs (a) to (d) of regulation 17(1)[89]; or
- where an enforcement notice was not served or where no steps were required to be taken under an enforcement notice, a failure described in one or more of sub-paragraphs (a) to (d) of regulation 17(1).

Our Penalty Guidelines

9.54 In determining penalties (including under regulation 18 of the Amended NIS Regulations), we will have regard to our Penalty Guidelines.[90] Section 392 of the Communications Act 2003 requires us to prepare and publish a statement containing the guidelines we propose to follow in determining the amount of penalties imposed by us under that Act or any other enactment (apart from the Competition Act 1998). The Amended NIS Regulations constitute such other enactment. We are therefore required[91] to have regard to the statement for the time being in force when setting the amount of any penalty also under the Amended NIS Regulations.

Our expected normal NIS enforcement approach where there are grounds for action

Contents of Section 4 of the Enforcement Guidelines

9.55 Section 4 of the Enforcement Guidelines mainly deals with the following matters:

- decision making in regulatory investigations;
- provisional breach notifications;
- written representations;
- oral hearings;
- further provisional breach notification;
- process for reaching a final decision;
- publication of final contravention decisions;
- case closure without a final contravention decision; and
- compliance monitoring.

9.56 Those matters are generally discussed in that Section 4 on the basis that Ofcom decides that there are grounds for pursuing formal enforcement action by issuing a 'provisional breach notification'.

---

[89] In other words, a failure to "*[…] (a) fulfil the security duties under regulation 10(1) and (2); (b) notify a NIS incident under regulation 11(1); (c) comply with the notification requirements stipulated in regulation 11(3);(d) notify an incident as required by regulation 12(9); […]*".

[90] https://www.ofcom.org.uk/about-ofcom/policies-and-guidelines/penalty-guidelines

[91] Section 392(6) of the Communications Act 2003.

Meaning of 'provisional breach notifications' under the Enforcement Guidelines

9.57 For most of our regulatory investigations covered by the Enforcement Guidelines, such a provisional breach notification typically envisages that:

- we first provide the subject of the investigation with a provisional decision explaining the reasons why we are minded to find a contravention of the relevant regulatory requirement(s) and the action(s) that we propose to take as a result;
- we include with any provisional breach notification our provisional view of the steps (if any) the subject should take to rectify the contravention;
- where we are minded to impose a financial penalty, we, include with any provisional breach notification, our provisional determination of the intended penalty; and
- we give the subject the opportunity to make representations before proceeding to take a final decision.

Our expected corresponding notices under the Amended NIS Regulations

9.58 We have already noted above that we have various choices available under the Amended NIS Regulations in terms of serving notices on OES. In particular, we can decide whether we simply inform an OES in accordance with regulation 17(2A) or whether we do so by providing the OES with a notice of our intention to serve an enforcement notice.

9.59 We can also choose to serve a notice of intention to impose a penalty or a penalty notice irrespective of whether we have served or are contemporaneously serving an enforcement notice on an OES under regulation 17(1). However, where we intend to serve a notice of intention to impose a penalty on an OES by reference to any failure of complying with its duty set out in regulation 17(3A), such a notice requires by its nature that we have already served an enforcement notice under regulation 17(1).

9.60 In line with our above-mentioned normal approach to provisional breach notifications for regulatory investigations covered by the Enforcement Guidelines, we expect in most cases to follow a similar approach under the Amended NIS Regulations, unless we decide that an alternative approach is appropriate given the facts and circumstances of specific cases. We will decide such cases on a case-by-case basis.

9.61 For example, as discussed in Section 6 of the Enforcement Guidelines, we have specific powers to take urgent action in relation to some types of enforcement action under other pieces of legislation, such as the Communications Act 2003. We may therefore from time to time rely on our powers to simply inform an OES in accordance with regulation 17(2A) of the Amended NIS Regulations, without serving a notice of our intention to serve an enforcement notice. In other cases, we may also decide to serve a notice of intention to impose a penalty without issuing an enforcement notice under regulation 17(1), as permitted under regulation 18(3C).

9.62 That said, where we follow our expected normal approach, we will contemporaneously serve a single document containing both:

- our notice of intention to serve an enforcement notice under regulation 17(2B), which will deal with the alleged failure and how and by when representations may be made in

relation to the alleged failure and any related matters (as required by regulation 17(2A); and

- if we intend to impose any penalty, our notice of intention to impose a penalty under regulation 18(1), which will include the matters specified in regulation 18(3).

9.63 Therefore, references to 'provisional breach notifications' in Section 4 of the Enforcement Guidelines should be read as references to such a single document of notifications in relation to our expected normal approach under the Amended NIS Regulations, unless the context otherwise requires.

9.64 In other cases where we do not intend to follow that normal approach, we will inform the subject of our investigation on a case-by-case basis how we will decide on the outcome of a regulatory investigation, who will make key decisions during an investigation and the related processes.

9.65 Annex A6 sets out an overview of our expected normal approach in taking enforcement action (and in imposing any penalties) under the Amended NIS Regulations, which is broadly aligned with how we approach regulatory enforcement cases under the Enforcement Guidelines.

Decision making in regulatory investigations

9.66 We discuss who makes key decisions in relation to provisional breach notifications during an investigation in paragraphs 4.5 and 4.6 of the Enforcement Guidelines. We will follow the same approach to decision making during an investigation under our above-mentioned expected normal approach under the Amended NIS Regulations.

Provisional breach notifications

9.67 We describe in paragraphs 4.7 to 4.9 of the Enforcement Guidelines how we would normally approach a provisional breach notification for regulatory investigations subject to the Enforcement Guidelines. Those paragraphs should be read in light of our above-mentioned expected normal approach under the Amended NIS Regulations.

9.68 In paragraph 4.10 of the Enforcement Guidelines, we explain that, if the subject of the investigation is a company, we will deliver the notification in hard copy to the Company Secretary and copied by email to our main contact, unless it has agreed otherwise with us.

9.69 Where we take any action under the Amended NIS Regulations (whether under our above-mentioned expected normal approach or otherwise), we will serve our notices in accordance with regulation 24.

9.70 Where the subject of our investigation is a company, regulations 24(1)(c) and 24(5)(a) permits us to serve our notice by post or electronic means to the registered or principal office of the company, or the email address of the secretary or clerk of that company. Where possible, we intend to serve our notices by using the email address of the Company Secretary. However, where an OES to whom regulation 8A of the Amended NIS Regulations applies, we will serve our notices by email on its nominated person that the OES has notified to Ofcom (see paragraphs 4.53 to 4.63 of this Guidance for further information

about nominated persons). In both cases, we will copy such an email to our main contact at the OES.

9.71 Paragraph 4.11 of the Enforcement Guidelines explains how we will make the evidence taken into account in reaching our provisional breach notification available to the subject of the investigation. We will make our evidence similarly available to an OES when we take our above-mentioned expected normal approach under the Amended NIS Regulations. In other cases, we will decide on a case-by-case basis what approach should be taken in that regard.

9.72 In paragraph 4.12 of the Enforcement Guidelines, we explain how we will mark any confidential information in the provisional breach notification (and any accompanying documents), together with any redactions of confidential third-party information. We expect to largely take a similar approach to any notices we serve under the Amended NIS Regulations (whether under our above-mentioned expected normal approach or otherwise). However, we reserve our position to adapt this approach, as appropriate, where it is relevant to share information with other authorities under regulation 6 of the Amended NIS Regulations.

9.73 Paragraph 4.13 of the Enforcement Guidelines explains that "*Ofcom will not publish provisional breach notifications but we will generally publish an update on the CCEB section of our website. Our update will normally explain that we have issued a provisional breach notification, include a summary of the proposed contraventions that we are minded to find and, where relevant, of the steps we propose the subject should take to comply and/or remedy the proposed contraventions. The CCEB update will also state that the subject will have the opportunity to make representations on our proposed findings before we make our final decision.*" We expect to do the same when we take our above-mentioned expected normal approach under the Amended NIS Regulations. In other cases, we will decide on a case-by-case basis what approach should be taken to publishing any information about the progress of our investigation.

Written representations

9.74 In paragraph 4.14 of the Enforcement Guidelines, we explain that the subject of the investigation will have the opportunity to make written representations to us on the proposed finding(s) and on any proposed penalty, proposed required steps and/or proposed direction. Such an opportunity will be given to an OES when we serve any notice of intention to serve an enforcement notice under regulation 17(2B) or notice of intention to impose a penalty under regulation 18(1), but not necessarily when we simply inform the OES in accordance with regulation 17(2A). We will decide on a case-by-case basis what approach should be taken in allowing an OES to make representations to us in the latter regard.

9.75 Paragraph 4.14 of the Enforcement Guidelines also states that typically we will give the subject a period of at least 20 working days for making written representations, and that we will give a longer period in more complex cases. While we will endeavour to give an OES at least 20 working days for making written representations to us in response to our

notices under the Amended NIS Regulations, we may give an OES a shorter period to do so, depending on the facts and circumstances (including urgency) of each case. However, we will always ensure that an OES is given a fair opportunity to consider our case against them (including our associated evidence) and to make representations to us.

9.76 Paragraphs 4.15 to 4.17 of the Enforcement Guidelines discuss how we may provide complainants or relevant third parties with the opportunity to comment on a non-confidential copy of the provisional breach notification. Those paragraphs are also relevant to our above-mentioned expected normal approach under the Amended NIS Regulations.

Oral hearings

9.77 Paragraphs 4.18 to 4.24 of the Enforcement Guidelines explain how we will offer the subject of the investigation the opportunity to attend an oral hearing to make oral representations on matters referred to in the provisional breach notification. Those paragraphs are also relevant to our above-mentioned expected normal approach under the Amended NIS Regulations. In other cases, we will decide on a case-by-case basis whether (and, if so, how) oral hearings should be offered to an OES whom we are investigating.

Further provisional breach notification

9.78 In paragraph 4.25 of the Enforcement Guidelines, we explain that, in some cases, new information or evidence may come to our attention after we have issued a provisional breach notification and given the subject of the investigation the opportunity to comment on it. We also explain that we will adopt an appropriate process to deal with such evidence which ensures fairness to the subject of the investigation.

9.79 Then, in paragraph 4.26, we clarify that, where such new information or evidence leads us to consider making a material change to the nature of the proposed contravention findings and/or increase the proposed level of penalty, we will withdraw the initial provisional breach notification and issue a new provisional breach notification. We also clarify that the subject would have the opportunity to comment on the new provisional breach notification as described above, before we proceed to reach a final decision.

9.80 We will follow the same approach as described in those paragraphs of the Enforcement Guidelines when we serve any notice of intention to serve an enforcement notice under regulation 17(2B) or notice of intention to impose a penalty under regulation 18(1) of the Amended NIS Regulations.

Process for reaching a final decision

9.81 Paragraphs 4.27 to 4.30 of the Enforcement Guidelines explain how we will take a final decision on a case. A similar process will be followed by us when we serve on an OES enforcement notices under regulation 17(1) or penalty notices with a final penalty decision under regulation 18(3A).

9.82 In paragraph 4.29 of the Enforcement Guidelines, we explain that, if the subject is a company, we will deliver the notification (with our final decision) in hard copy to the Company Secretary, copied by email to our main contact, unless it has agreed otherwise with us. Again, as already explained in paragraph 9.70 above, we will serve our notices in accordance with regulation 24 and follow the same approach as described in that paragraph where the subject of our investigation is a company.

Publication of final contravention decisions

9.83 Paragraphs 4.31 and 4.32 of the Enforcement Guidelines explain what we will do once we have made our final contravention decision, including what we publish on our website (www.ofcom.org.uk). Those paragraphs will apply also to any final decisions on enforcement action or penalties that we reach under the Amended NIS Regulations.

Case closure without a final contravention decision

9.84 Paragraphs 4.33 to 4.38 of the Enforcement Guidelines explain the process we will follow when we conclude that we should not take any further action and close the case. That process will also apply to any case closure without serving any enforcement notice or penalty notice under the Amended NIS Regulations.

9.85 Additionally, as already noted above, we will inform an OES in writing as soon as reasonably practicable in accordance with regulation 17(4), if we are satisfied that no further action is required having considered any representations submitted by the OES in accordance with regulation 17(2A) or any steps taken by the OES to rectify the alleged failure. Where requested by the OES pursuant to regulation 17(5), we will provide the OES with our written reasons for our decision for taking no further action within a reasonable time and, in any event, no later than 28 days in accordance with regulation 17(6).

Compliance monitoring

9.86 Paragraphs 4.39 to 4.43 of the Enforcement Guidelines explain that we may decide to pursue compliance monitoring in certain cases. Those paragraphs will apply also to any enforcement action we take, or case closure we make based on accepted assurances from an OES, under the Amended NIS Regulations.

9.87 In paragraph 4.40 of the Enforcement Guidelines, we mention that we may use our information gathering powers in order to obtain information to assess compliance. Our compliance phase under the Amended NIS Regulations may involve using our powers under regulation 15 to serve information notices on an OES and, where appropriate, we may also supplement such information gathering by conducting inspections under regulation 16, which we discuss separately in Section 8 of this Guidance.

Settlement procedure

9.88 Section 5 of the Enforcement Guidelines discusses our settlement procedure for those cases which we decide are suitable for settlement. That settlement procedure will also

apply where we are intending to impose a penalty on an OES under the Amended NIS Regulations.

9.89 It is important to note, as explained in that Section 5, that those who we are investigating are not under any obligation to enter into a settlement process or to settle, and we have broad discretion to decide whether a case is appropriate for settlement or to agree to settlement.

9.90 Also, settlement is not a negotiation with us about what contraventions we might be prepared to find or not to find. Nor is it a negotiation about the level of the intended penalty which we would impose, nor is it equivalent to the type of discussions which take place between parties to litigation or potential litigation on a "without prejudice" basis for the purposes of seeking to resolve or avoid litigation.

9.91 We discuss, in particular, the following matters in Section 5 of the Enforcement Guidelines:

- requirements for settlement;
- how we decide whether a case is suitable for settlement;
- settlement discounts;
- decision-making in a settlement case; and
- the settlement process.

9.92 In doing so, we particularly explain that the level of discount on the level of penalty we intend to impose as a result of settlement will depend on the stage at which a successful settlement process is commenced. Where we refer in Section 5 of the Enforcement Guidelines to stages falling prior to, or following, provisional breach notifications, such references should be read as references to stages falling prior to, or following, us serving any notices of intention to impose a penalty on an OES under regulation 18(1) of the Amended NIS Regulations, irrespective of whether we have served or are contemporaneously serving an enforcement notice on the OES under regulation 17(1).

Procedural complaints about investigations

9.93 Section 9 of the Enforcement Guidelines explains how we will deal with any complaint by the subject of an investigation, any complainant or a third party (where relevant) who is dissatisfied about any aspect of our investigation procedure.

9.94 Those processes (including the making of a complaint to Ofcom's Procedural Officer) also apply when we conduct an investigation under regulation 17 and impose any penalties under regulation 18 of the Amended NIS Regulations.

10. Details of the appeals process

10.1 We explain in Section 9 of this Guidance that our penalty notices with a final penalty decision must (among other things) provide details of the appeal process under regulation 19A of the Amended NIS Regulations.

10.2 In this section, we provide the details of that appeal process.

Appealable decisions under regulation 19A

10.3 Regulation 19A(1) provides that an OES may appeal to the First-tier Tribunal against one or more of the following decisions made by us:

- a decision under regulation 8(3) to designate that person as an OES;
- a decision under regulation 9(1) or (2) to revoke the designation of that OES;
- a decision under regulation 17(1) to serve an enforcement notice on that OES;
- a decision under regulation 18(3A) to serve a penalty notice on that OES.

10.4 Regulation 1(2) of the Amended NIS Regulations defines "First-tier Tribunal" as having the meaning given by section 3(1) of the Tribunals, Courts and Enforcement Act 2007. It should also be noted that the transitional and saving provisions set out in regulation 21 of the Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 refer to the Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (the "2009 Rules").

10.5 Our understanding is that the First-tier Tribunal (General Regulatory Chamber) (the "GRC") will handle the above-mentioned appeals and that its 2009 Rules will apply in that regard.

Grounds of appeal under regulation 19A

10.6 Regulation 19A(1) also provides that an OES may only appeal the above-mentioned decisions on one or more of the grounds specified in regulation 19A(3) of the Amended NIS Regulations, namely:

- that the decision was based on a material error as to the facts;
- that any of the procedural requirements under the Amended NIS Regulations in relation to the decision have not been complied with and the interests of the OES have been substantially prejudiced by the non-compliance;
- that the decision was wrong in law;
- that there was some other material irrationality, including unreasonableness or lack of proportionality, which has substantially prejudiced the interests of the OES.

Starting proceedings before the GRC

10.7 The means of making an appeal is by sending or delivering to the GRC a notice of appeal in accordance with 2009 Rules.

Time limit for appealing to the GRC

10.8 Rule 22(1) of the 2009 Rules provides that an appellant must start proceedings before the GRC by sending or delivering to the GRC a notice of appeal so that it is received by the GRC within 28 days of the date on which notice of the decision to which the proceedings relate was sent to the appellant by Ofcom.

10.9 In relation to that 28-day deadline, it should also be noted that rule 12 of the 2009 Rules makes provisions for calculating time, in particular:

- an act required by the 2009 Rules, a practice direction or a direction to be done on or by a particular day must be done before 5pm on that day;
- if the time specified by the 2009 Rules, a practice direction or a direction for doing any act ends on a day other than a working day[92], the act is done in time as if it is done on the next working day.

Contents of the notice of appeal

10.10 Rule 22(2) states that the notice of appeal must include:

- the name and address of the appellant;
- the name and address of the appellant's representative (if any);
- an address where documents for the appellant may be sent or delivered;
- the name and address of any respondent;
- details of the decision to which the proceedings relate;
- the result the appellant is seeking;
- the grounds on which the appellant relies; and
- any further information or documents required by a practice direction.

10.11 Rule 22(3) further provides that, if the proceedings challenge a decision, the appellant must provide with the notice of appeal a copy of any written record of that decision, and any statement of reasons for that decision that the appellant has or can reasonably obtain.

Sending a copy of the notice of appeal to us

10.12 Rule 22(5) explains that, when the GRC receives the notice of appeal, subject to rule 19(1A) (national security appeals), the GRC must send a copy of the notice of appeal and any accompanying documents to the respondent.

10.13 While the GRC is responsible under that rule to send a copy of the notice of appeal (and any accompanying documents) to Ofcom (as the respondent), we request that the appellant also sends a PDF copy of that notice of appeal by email to us at nis@ofcom.org.uk, at the same time as the appellant sends it to the GRC pursuant to rule 22(1) or as soon as possible thereafter.

[92] Rule 12(3) of the 2009 Rules defines "working day" as meaning any day except a Saturday or Sunday, Christmas Day, Good Friday or a bank holiday under section 1 of the Banking and Financial Dealings Act 1971.

Our response to the notice of appeal

10.14 Rule 23 makes provision about the response to the notice of appeal. In particular, it provides that each respondent must send or deliver to the GRC a response to the notice of appeal so that it is received within 28 days after the date on which the respondent received the notice of appeal.

Information for potential appellants

10.15 We recommend that anyone seeking to appeal against an appealable decision by Ofcom to the GRC considers all relevant practice directions, guides and other updates published from time to time in relation to proceedings before the GRC. As a starting point, we recommend that parties consider any information published on the gov.uk webpage for the GRC.[93]

10.16 We also recommend that parties carefully consider HM Court & Tribunals Service's document entitled 'T97 Guide to completing the notice of appeal General Regulatory Chamber (GRC)(10.19)'. You will note that it requests that an appellant uses the notice of appeal form ('T98 Notice of appeal (05.19)'), which can be downloaded from https://www.gov.uk/government/publications/form-t98-notice-of-appeal-general-regulatory-chamber-grc

10.17 That guide also requests (among other things) that the signed, dated and completed notice of appeal is sent to:

General Regulatory Chamber

HM Courts & Tribunals Service

PO Box 9300

Leicester

LE1 8DJ

email: grc@justice.gov.uk

10.18 The GRC can also be reached by telephone on 0300 123 4504.

10.19 We also note the 'Update on Ways of Working in the GRC – June 2020'[94] by the Chamber President, Judge Alison McKenna, contains some useful practical information about the GRC's new ways of working in light of the COVID 19 Pandemic.

Sending and delivery of documents to Ofcom

10.20 Rule 13 of the 2009 Rules makes provision about sending and delivery of documents. It provides:

[93] https://www.gov.uk/courts-tribunals/first-tier-tribunal-general-regulatory-chamber
[94] https://www.judiciary.uk/wp-content/uploads/2020/06/GRC-June-update-002-1.pdf

"*(1) Any document to be provided to the Tribunal under these Rules, a practice direction or a direction must be—*

(a) sent by prepaid post or by document exchange, or delivered by hand to the address specified for the proceedings;

(b) sent by fax to the number specified for the proceedings; or

(c) sent or delivered by such other method as the Tribunal may permit or direct.

(2) Subject to paragraph (3), ***if a party provides*** *a fax number,* ***email address*** *or other details for the electronic transmission of documents to them,* ***that party must accept delivery of documents by that method****.*

(3) If a party informs the Tribunal and all other parties that a particular form of communication, other than pre-paid post or delivery by hand, should not be used to provide documents to that party, that form of communication must not be so used.

(4) ***If the Tribunal or a party sends a document to a party or the Tribunal by email or any other electronic means of communication, the recipient may request that the sender provide a hard copy of the document to the recipient****. The recipient must make such a request as soon as reasonably practicable after receiving the document electronically.*

(5) The Tribunal and each party may assume that the address provided by a party or its representative is and remains the address to which documents should be sent or delivered until receiving written notification to the contrary." (emphasis added)

Our request to the GRC, appellants and any third parties to an appeal

10.21 In light of rule 13 of the 2009 Rules, we request that, unless we notify in writing otherwise, the GRC, appellants and any other third parties to an appeal send and deliver documents to Ofcom in the following manner:

— send by prepaid post or deliver by hand **a hard copy** of every document in relation to an appeal to: **General Counsel, Legal Group, Office of Communications, Riverside House, 2a Southwark Bridge Road, London, SE1 9HA**

AND

— send a **PDF copy** of such a hard copy **by email** with a subject line of "GRC documents" to nis@ofcom.org.uk

Decision of the First-tier Tribunal (GRC)

10.22 Regulation 19B(1) of the Amended NIS Regulations provides that the First-tier Tribunal (i.e. the GRC) must determine the appeal after considering the grounds of appeal referred to in regulation 19A(3) and by applying the same principles as would be applied by a court on an application for judicial review.

10.23 The GRC may confirm any decision to which the appeal relates or quash the whole or part of any decision to which the appeal relates.[95] Where the GRC quashes the whole or part of a decision to which the appeal relates, it must remit the matter back to Ofcom, with a direction to Ofcom to reconsider the matter and make a new decision having regard to the GRC's ruling.[96] We must have regard to such a direction.[97] Where we make a new decision in accordance with such a direction, that decision is to be considered final.[98]

10.24 Regulation 19B(2) also provides that the GRC may, until it has determined the appeal and unless the appeal is withdrawn, suspend the effect of the whole or part of any appealable decision. In that regard, it should be noted that rule 20 of the 2009 Rules sets out the procedure for applying for a stay of a decision pending an appeal, including that the appellant must make a written application to the GRC in accordance with the rule.

[95] Regulation 19B(3).
[96] Regulation 19B(4).
[97] Regulation 19B(5).
[98] Regulation 19B(6).

11. Our approach to cost recovery

OES duty to pay our NIS functions fees

Statutory duty to pay our fees

11.1 Regulation 21(1) imposes the following statutory duty on OES to pay our NIS functions fees:

> *"A fee is payable by an OES […] to an enforcement authority, to recover the reasonable costs incurred by, or on behalf of, that authority in carrying out a NIS function in relation to that OES […]."*

11.2 We have, however, the power to determine not to charge a fee under regulation 21(1) in any particular case.[99]

Deadline for paying our fees

11.3 Regulation 21(2) imposes a requirement on OES to pay the fee mentioned in regulation 21(1) "*within 30 days after receipt of the invoice sent by the authority*".

11.4 In other words, the 30-day period for paying our fees commences on the day an OES receives our invoice.

Our recoverable costs

Reasonable costs of our "NIS functions"

11.5 As explained above, we can only recover our reasonable costs in carrying out a NIS function in relation to an OES. The concept of a "NIS function" is defined in regulation 21(6)(a) as:

> *"a "NIS function" means a function that is carried out under these Regulations except any function under regulations 17(1) to (4) and 18 to 20;"*

11.6 In other words, we can recover under regulation 21 our reasonable costs in carrying out all of our functions under the Amended NIS Regulations, apart from any costs we incur in carrying out the following functions (we refer to them below as "excluded functions"):

- serving enforcement notices on OES under regulation 17;
- imposing any penalties on OES under regulation 18;
- dealing with any appeals under regulations 19A and 19B;
- enforcing requirements of enforcement notices by civil proceedings under regulation A20; and
- enforcing penalty notices under regulation 20.

[99] Regulation 21(4).

11.7 We have already noted earlier in this Guidance (see, in particular, Section 2) our main duties and powers in relation to the digital infrastructure subsector under the Amended NIS Regulations. We carry out such functions—in relation to which we may recover our reasonable costs (which are not excluded functions)—when we (for example):

- periodically review the application of the Amended NIS Regulations in conjunction with DCMS and others;
- prepare and publish guidance;
- administer OES designations.

Our approach to cost allocation

11.8 To satisfy the requirements of regulation 21 (additionally to ensuring a fair cost allocation among OES), our approach involves us firstly breaking down our recoverable costs into three broad categories, namely:

- **Category 1 costs**: Costs allocated to this category are costs for generic work we have done in carrying out our NIS functions, which are not specific to any OES; as such they do not include our costs in carrying out our excluded functions. However, they typically include costs relating to our work such as reviewing the application of the Amended NIS Regulations; preparing, updating and publishing guidance for this subsector; keeping lists of OES and related administration; and consulting and co-operating with various other regulatory bodies and authorities.
- **Category 2 costs:** Costs allocated to this category are costs for specific work we have done in relation to a specific OES. Again, they do not include our costs in carrying out our excluded functions. However, they could include costs we incur in relation to a specific OES such as in dealing with their individual incident engagements, designations and information notice(s) served under regulation 15.
- **Category 3 costs:** Costs allocated to this category include common costs such as finance & HR. These costs are proportionately allocated to all our regulatory sectors. This cost category excludes our costs in carrying out our excluded functions.

How we allocate Category 1 costs (Generic costs)

11.9 The total cost of Category 1 costs is divided equally amongst all the OES falling within the digital infrastructure subsector.

How we allocate Category 2 costs (OES specific costs)

11.10 We allocate the total cost of Category 2 costs (if any) to each of the relevant OES.

11.11 In other words, if we have not undertaken any work in relation to a specific OES, the amount we allocate for Category 2 costs to that OES will be zero.

How we allocate Category 3 costs (Common costs)

11.12 A proportion of the common costs is allocated to the NIS programme of work and divided equally among all the OES falling within the digital infrastructure subsector.

How we work out the total invoiced fee for each OES

11.13 Based on the above, the total fee invoiced to a specific OES is calculated as follows:

$$OES\ fee = \frac{Total\ of\ category\ 1{+}3\ costs}{Number\ of\ OES\ in\ scope\ as\ of\ 31\ March} + Category\ 2\ costs$$

Our invoices to OES

Contents of our invoices

11.14 Regulation 21(3) provides:

> *"The invoice must state the work done and the reasonable costs incurred by, or on behalf of, the enforcement authority, including the time period to which the invoice relates."*

11.15 In relation to the work we have done and our associated reasonable recoverable costs, our invoices will not be itemised in terms of detailed costs we have incurred (e.g. worked hours, chargeable hourly rates etc).

Charging period

11.16 In relation to the time period to which our invoices relate, we normally issue invoices in arrears on an annual basis covering a 12-month period. Our financial year runs from 1 April to 31 March, and we expect to normally send OES our invoices as soon as possible after 31 March each year.

11.17 In other words, our invoice period will reflect our recoverable costs incurred in the previous 12-month period covering 1 April to 31 March. For example:

- Our financial year: 1 April 2020 to 31 March 2021
- Our invoice period: 1 April 2019 to 31 March 2020

How we will invoice OES

11.18 Our invoices will be sent to the contact address of the OES with an accompanying letter providing additional information as necessary.

OES payment of our invoices

11.19 We have already noted above that the deadline for paying our fees is 30 days after receipt of our invoice.

11.20 Acceptable payment methods will be explained in our invoices.

11.21 Once an OES has paid our invoice, we request that the OES notifies us by emailing all relevant details e.g. (OES name, amount, invoice number etc.) to ofcom.remittances@ofcom.org.uk along with proof of payment.

Consequences of failure to pay us

11.22 Regulation 21(5) provides that a fee payable under this regulation is recoverable as a civil debt.

11.23 Accordingly, we will issue civil proceedings if we do not receive payment for our invoices before the deadline for payment.

A1. Contacting our NIS team

General contact details

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

Switchboard: 0300 123 3000 or 020 7981 3000

Incident reporting only

Email incident@ofcom.org.uk with incident reports: see Section 5 of this Guidance for further information about the manner and form for reporting incidents to us.

Freedom of Information (FOI) requests

Our details for how to make an FOI request is available here: https://www.ofcom.org.uk/about-ofcom/foi-dp/make-foi-request

Our postal address

Network and Information Systems (NIS) Team
Networks & Communications Group
The Office of Communications
Riverside House
2a Southwark Bridge Road
London
SE1 9HA

A2. Incident reporting

Ofcom NIS Incident Report Form (template)

	Ofcom NIS Incident Report Form	
1	OES name and the essential service it provides	
2	OES incident reference number	
3	Date, time and time zone of incident occurrence	
4	Date, time and time zone of incident resolution	
5	Service impact duration	
6	Location / geographic spread of impact	
7	Informed SPOCs	
8	Description of incident	
9	Primary Root cause: Select one of: System failure Natural phenomena Human error Malicious action Third party failure Other (please specify)	
10	NCSC Cyber Attack Categorisation[100] Select one of: C1 / C2 / C3 / C4 / C5 / C6 / Not a cyber attack	
11	Incident Severity Select one of: High / Medium / Low	
12	Incident Impact: Select one of: Red / Yellow / Green / White	
13	Impact on economic and societal activities Select one of: Red / Yellow / Green / White	
14	Action taken: Please include information regarding any remedial action taken, and any other competent authorities, or CSIRTs, from either the UK, or EU states, that have been notified.	
15	Name and contact details for follow up questions	

[100] https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents

Ofcom's Guidance for completing the NIS Incident Report Form

The remainder of this annex provides our explanations and guidance for OES which they must consider in completing our NIS incident report form (template) set out above.

Row 1: OES name and the essential service it provides

The full name of the OES and the essential service it provides.

Row 2: OES incident reference number

If the OES has allocated any of its own incident reference number for internal use, such a reference number should be given to Ofcom.

Row 3: Date, time and time zone of incident occurrence

The date, time and time zone when the incident met or exceeded the NIS incident reporting threshold.

In the case of a voluntary reported incident which has not exceeded a NIS incident reporting threshold, the date, time and time zone when the incident first occurred.

Row 4: Date, time and time zone of incident resolution

The date, time and time zone when the incident was resolved or when services are fully recovered.

Row 5: Service impact duration

The period of time for which the essential service is unavailable or of degraded availability. This information will assist in determining the severity of impact.

Row 6: Location and geographic spread of impact

The city, county or country affected. An OES must inform us which member state(s) are affected if there is any cross-border impact.

Row 7: Informed SPOCs

OES may need to inform more than one SPOC in some types of incident. For example, an OES may need to inform the SPOCs in other EU member states if an incident has cross-border impact.

Row 8: Description of incident

Description of the incident regarding what has happened and an initial statement of probable cause.

If an OES is reliant on a RDSP to provide an essential service and significant impact on the continuity of the RDSP service is the probable cause or contributor to the incident, the following information should be included in the description:

- the RDSP name and the essential services that were affected;

- the time the RDSP incident occurred;
- the duration of the RDSP incident (This would be provided in the OES PIR);
- information concerning the nature and impact of the RDSP incident;
- information concerning any, or any likely, cross-border impact of the RDSP incident; and
- any other information that may be helpful to Ofcom.

Row 9: Primary root cause

A Root Cause is the fundamental reason why an incident occurred. Please select one of the six mutually exclusive root causes listed below.

System failure	The incident is due to the failure of a system i.e. without external causes for example a hardware failure, software bug or flaw in a procedure etc.
Natural phenomena	The incident is due to a natural phenomenon for example a storm, lightning, solar flare, flood, earthquake or wildfire etc.
Human error	The incident is due to human error i.e. the system worked correctly but was used in an incorrect manner for example a mistake or carelessness triggered the incident.
Malicious actions	The incident is due to a malicious action or actions for example a cyber-attack or physical attack, vandalism, sabotage, insider attack or theft etc.
Third party failures	The incident is due to disruption of a third-party service like a utility for example a power cut or an Internet outage triggered the incident.
Other (please specify)	If none of the above-mentioned root causes apply, please specify the nature of the root cause.

Row 10: NCSC's cyber attack categorisation

The NCSC classifies cyber attacks into six categories to improve incident response and resource allocation; details, including the definition of the six categories, can be found on NCSC's website[101]. An OES only needs to select one of the six categories if the incident involves a cyber attack element otherwise the OES should state "Not a cyber attack".

Row 11: Incident severity

The severity of an incident indicates the impact of the incident from a technical perspective on the OES. Factors to consider may include:

- the amount of additional effort or costs needed to mitigate, protect or recover from the incident;
- the criticality of the systems affected (e.g. mission-critical SCADA systems);
- the feasibility or availability of solutions or protection measures which mitigate the threat;

[101] https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents

and

- adequacy of industry standards and industry best practices in mitigating the threat.

OES should assess the incident severity using the criteria set out in the table below. An incident falls within a given category if one or more of the criteria are met.

Table: Criteria of different level of incident severity

Incident Severity	Criteria
High	• Costs greater than £100,000 will be incurred to resolve the incident • There are unrecoverable damages for example, data theft or data loss. • There was disruption to critical services. • No immediate solution is available
Medium	• Costs of between £5,000 and £100,000 will be required to resolve the incident. • There are no unrecoverable damages for example, data theft or data loss. • Critical services are not affected.
Low	• Costs less than £5,000 will be required to resolve the incident. • There are no unrecoverable damages for example, data theft or data loss. • Service availability was not affected.

Row 12: Incident impact

Incident impact indicates the scale of impact of the incident on the economy and society. This includes (but is not limited to):

- Risks to the health and safety of the population, for example affecting emergency services;
- Damages and costs for citizens and/or organizations affected;
- Disruption of daily life;
- Cascading effects in critical sectors;
- Media impact and coverage; and
- Political impact and significance.

OES should assess the incident impact into one of the four possible categories using the criteria set out in the table below. An incident falls within a given category if one or more of the criteria are met.

Table: Criteria for different level of incident impact

Indicator	Criteria
Red (High)	• The extent of the disruption and proportion of users affected falls within the red zone in the table below. • Cross-border impacts have occurred. • Damages and remedy costs totalling £100,000 or more. • There are cascading effects in multiple critical sectors.

Yellow (Medium)	• The extent of the disruption and proportion of users affected falls within the yellow zone in the table below. • Cross-border impacts have occurred. • Damages and costs totalling £5,000 or more but less than £100,000. • There are cascading effects in multiple non-critical sectors.
Green (Low)	• The extent of the disruption and proportion of users affected falls within the green zone in the table below. • There are no cross-border impacts. • Damages and costs totalling £1,000 or more but less than £5,000. • There are no cascading effects in other sectors.
White (Baseline)	• The extent of the disruption and proportion of users affected falls within the white zone in the table below. • There are no cross-border impacts. • Damages and costs totalling less than £1,000. • There are no cascading effects in other sectors. • Just met the NIS reporting thresholds (Refer to the latest NIS Guidance).

Row 13: Relative threshold for impact on economic and societal activities

Economic and societal activities impact refer to the possible damage to the national or international market. It may be difficult for an OES to determine the impact because they normally could not obtain the information required for evaluating the impact.

The table below show the relative threshold for high (red), medium (yellow), low (green) and baseline (white) impact on economic and societal activities.

Relative threshold for impact on economic and societal activities

Relative Threshold		Critical Service Impact						
		0 to 1 hours	1 to 2 hours	2 to 4 hours	4 to 6 hours	6 to 8 hours	8 to 10 hours	10+ hours
Percentage of consumers affected	0% to 2%							
	2% to 5%							
	5% to 10%							
	10% to 15%							
	15%+							

Row 14: Action taken

Please include information regarding any remedial action taken, and any other competent authorities, or CSIRTs, from either the UK, or EU states, that have been notified.

Row 15: Name and contact details for follow up questions

Please include the name and contact details of a person able to receive and respond to follow up questions.

A3. Glossary

Abbreviation	Meaning
CAF	Cyber Assessment Framework
CSIRT	Computer Security Incident Response Team
DCMS	Digital, Culture, Media & Sport
DNS	Domain Name System
EU	European Union
GCHQ	Government Communications Headquarters
GRC	General Regulatory Chamber
IXP	Internet Exchange Point
NCSC	National Cyber Security Centre
NIS	Network and Information Systems
OES	Operator of an Essential Service
PIR	Post Incident Report
RDSP	Relevant Digital Service Provider
SPOC	Single Point of Contact
TLD	Top Level Domain
UK	United Kingdom

A4. Our previous guidance on potential regulatory overlap for DNS Resolver Services

Introduction

A4.1 New regulation 8(1A) of the Amended NIS Regulations explains that regulation 8(1) does not apply to a network provider or service provider[102] who is subject to the requirements of sections 105A to 105C of the Communications Act 2003.

A4.2 Article 1(3) of the NIS Directive contains a corresponding provision to regulation 8(1A): "*3. The security and notification requirements provided for in this Directive shall not apply to undertakings which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC, or to trust service providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014.*"[103]

A4.3 Some communications providers queried with Ofcom at the time of their OES notifications in 2018 whether they should, in fact, be notifying themselves for the purpose of regulation 8(1) of the NIS Regulations in light of their requirements under the section 105A of the Communications Act 2003 in relation to DNS resolvers.

A4.4 In light of those queries, we wrote in 2018 to affected communications providers setting out our specific guidance on how we consider that the NIS Regulations and the section 105A regime should apply respectively, in principle, in relation to the DNS Resolvers Services described in paragraph 10(3)(a) of Schedule 2 to the NIS Regulations. We summarise that guidance below.

Potential overlap with the Framework Directive for DNS resolvers

A4.5 We started our guidance by noting that the requirements of Articles 13a and 13b of Directive 2002/21/EC (known as the "Framework Directive") have the potential to capture also DNS resolvers offered for use by publicly accessible services, such as publicly available electronic communications services in the form of internet access services ("IAS").

A4.6 This was because an IAS is a service[104] that falls within the definition of an 'electronic communications service' ("ECS").

---

[102] The concepts of "network provider" and "service provider" have the meanings given in section 105A(5) of the Communications Act 2003.

[103] Sections 105A to 105D of the Communications Act 2003 implement Articles 13a and 13b of Directive 2002/21/EC.

[104] At the time of giving our specific guidance, we noted that the provision of an IAS is an express example of an ECS given in recital (10) to the preamble of the Framework Directive. However, Directive 2018/1972/EU establishing the European Electronic Communications Code (the "EECC") has since repealed the Framework Directive with effect from 21 December 2020. Article 40 of the EECC now instead contains similar requirements to those under Article 13a and 13b of the Framework Directive, and they remain applicable to providers of public electronic communications networks or of publicly available electronic communications services. In that regard, Article 2(4) of the EECC also contains a new ECS definition, which refers to an 'internet access service'—as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120—as a specific type of ECS. A corresponding new ECS definition now applies under section 32(2A)(a) of the

A4.7 Therefore, we noted that, if the IAS is provided so as to be available for use by members of the public (i.e. a publicly available ECS), its provider is, as a starting point, subject to the requirements of Articles 13a and 13b of the Framework Directive.

A4.8 We explained that, in our understanding, IAS are not typically provided without the associated provision of a DNS Resolver Service. This is because for the majority of customers the IAS would be impractical to use without a DNS resolver in order to properly access and use the Internet. While it is technically and theoretically possible to do provide an IAS without a DNS resolver, we believed that, even if such a service was offered or provided by anyone, it is likely to be rare and used only by sophisticated niche customers.

A4.9 Our understanding was also that:

a) some internet service providers ("ISPs") had technical measures in place to actively prevent their customers from changing their own default DNS resolvers in customers' broadband routers; and

b) while other ISPs did not prevent their customers from changing their own default DNS resolvers as such, they discouraged their customers from doing so for various reasons.

A4.10 Accordingly, we considered that ISPs' provision of their default DNS resolvers is normally inextricably linked with, and forms an integral part of, the provision of the IAS itself. As such, we considered that both such IAS and its associated DNS resolver service are subject to the requirements of Articles 13a and 13b of the Framework Directive, which have been implemented in the United Kingdom by sections 105A to 105D of the Communications Act 2003.

A4.11 While there was no express provision[105] in the NIS Regulations reflecting the above-mentioned in Article 1(3) of the NIS Directive at the time we gave our above-mentioned specific guidance, we noted that the provision in Article 1(3) needs to be read into the application of the NIS Regulations. We noted in particular that such an approach followed from the so-called *Marleasing* principle in "*that, in applying national law, whether the provisions in question were adopted before or after the directive, the national court called upon to interpret it is required to do so, as far as possible, in the light of the wording and the purpose of the directive in order to achieve the result pursued by the latter and thereby comply with the third paragraph of Article 189 of the Treaty*" (paragraph 8, European Court of Justice's judgment in Case C-106/89).

Other DNS resolvers potentially subject to the requirements in the NIS regulations

A4.12 In contrast to above-mentioned DNS resolvers provided by ISPs, we explained that other DNS resolvers offered for use by publicly accessible services, such as those offered by some companies as a free-standing public DNS resolution service (without the provision of any

Communications Act 2003, see the Electronic Communications and Wireless Telegraphy (Amendment) (European Electronic Communications Code and EU Exit) Regulations 2020 (SI 2020/1419).

[105] Regulation 8(1A) of the Amended NIS Regulations now contains such express provision.

associated IAS), are potentially subject to the requirements under the NIS regulations, if the applicable threshold requirement in paragraph 10(3)(a) of Schedule 2 to the NIS Regulations was met.

A4.13 Accordingly, we explained that our intention was to investigate and enforce any compliance of such other DNS Resolver Services with the requirements under the NIS Regulations.

A5. Version history

A5.1 The table below sets out the date and effect of changes that have been made to this Guidance in order to assist users in accessing the most up-to-date version of this Guidance.

Date of publication	Provision(s) affected in this Guidance	Summary of change(s) & effective date(s)	Name & published location
8 May 2018	All	Initial guidance published. Effective from 20 June 2018.[106]	Ofcom's interim guidance for Operators of Essential Services in the digital infrastructure subsector under the Network and Information Systems Regulations 2018. https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/guidance-network-information-systems-regulations
4 January 2021	Paragraph 4.36 (deemed OES) and paragraph 4.59 (nominated person)	Interim note to explain how to notify Ofcom of deemed OES designations and nominated persons (for non-UK based OES). Effective from 4 January 2021.	Update January 2021 https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/guidance-network-information-systems-regulations/update-january-2021
5 February 2021	All	Guidance was updated in its entirety to reflect changes introduced by the Amended NIS Regulations. Effective from 5 February 2021. This Guidance replaces our initial guidance and 4 January 2021 Update.	Guidance for the digital infrastructure subsector – Statutory guidance under the Network and Information Systems Regulations 2018: NIS Guidance https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/guidance-network-information-systems-regulations

[106] While the NIS Regulations came into force on 10 May 2018, regulation 8(2) omitted to make reference to paragraph 10 of Schedule 2 to the NIS Regulations, which meant that no deemed designations of OES for the digital infrastructure subsector were in place until regulation 2(5) of the Network and Information Systems (Amendment) Regulations 2018 (S.I. 2018/629) corrected that omission (which came into force on 20 June 2018).

A6. Overview of a typical regulatory enforcement case