Changes to legislation: *There are currently no known outstanding effects for the The Network and Information Systems Regulations 2018. (See end of Document for details)*

STATUTORY INSTRUMENTS

2018 No. 506

ELECTRONIC COMMUNICATIONS

The Network and Information Systems Regulations 2018

Made - - - -	*19th April 2018*
Laid before Parliament	*20th April 2018*
Coming into force - -	*10th May 2018*

The Secretary of State is a Minister designated [M1] for the purposes of section 2(2) of the European Communities Act 1972 [M2] ("the 1972 Act") in relation to electronic communications.

These Regulations make provision for a purpose mentioned in section 2(2) of the 1972 Act and it appears to the Secretary of State that it is expedient for certain references to provisions of EU instruments to be construed as references to those provisions as amended from time to time.

The Secretary of State makes the following Regulations in exercise of the powers conferred by section 2(2) of, and paragraph 1A [M3] of Schedule 2 to, the 1972 Act and by section 56 of the Finance Act 1973 [M4] ("the 1973 Act") and, in the case of section 56 of the 1973 Act, with the consent of the Treasury.

Marginal Citations

M1 S.I. 2001/3495. See article 2 of, and Schedule 1 to, these Regulations. There are amendments not relevant to these Regulations.

M2 1972 c.68. Section 2(2) was amended by section 27(1)(a) of the Legislative and Regulatory Reform Act 2006 (c.51) and by Part 1 of the Schedule to the European Union (Amendment) Act 2008 (c.7). In so far as these Regulations deal with matters that are within the devolved competence of Scottish Ministers, the power of the Secretary of State to make regulations in relation to those matters in or as regards Scotland is preserved by section 57(1) of the Scotland Act 1998 (c.46).

M3 Paragraph 1A of Schedule 2 was inserted by section 28 of the Legislative and Regulatory Reform Act 2006 and amended by Part 1 of the Schedule to the European Union (Amendment) Act 2008 and by article 3 of and paragraph 1 of Schedule 1 to SI 2007/1388.

M4 1973 c.51. Section 56 was amended by S.I. 2011/1043; there are other amendments not relevant to these Regulations.

PART 1

Introduction

Citation, commencement, interpretation and application

1.—(1) These Regulations may be cited as the Network and Information Systems Regulations 2018 and come into force on 10th May 2018.

(2) In these Regulations—

"cloud computing service" means a digital service –

(a) that enables access to a scalable and elastic pool of shareable computing resources; (such as networks, servers, software and storage) where –

(i) there is a broad remote access to the service,

(ii) the service is capable of being provided on demand and on a self-service basis,

(iii) the pool of computing resources may be distributed across two or more locations, and

(iv) the service is not provided by a person solely for use for the purposes of a business or other activity carried on for that person, and

(b) which is not a managed service. *[(7) Digital Services]*

"the Commission" means the Commission of the European Union;

[[F1]"EU Regulation 2018/151" means Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact;**]**

"Cooperation Group" means the group established under Article 11(1);

"critical supplier" means a person for the time being designated under regulation 14H; *[(12) Critical Suppliers]*

"CSIRTs network" means the network established under Article 12(1);

~~"digital service" means a service within the meaning of point (b) of Article 1(1) of Directive 2015/1535 which is of any the following kinds –~~

~~(a) online marketplace;~~

~~(b) online search engine;~~

~~(c) cloud computing service;~~

~~"digital service provider" means any person who provides a digital service;~~ *[(7) Digital Services]*

"Directive 2013/11" means Directive 2013/11/EU of the European Parliament and of the Council on alternative dispute resolution for consumer disputes [M5], and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC, as amended from time to time;

"Directive 2015/1535" means Directive (EU) 2015/1535 of the European Parliament and of the Council laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [M6], as amended from time to time;

"Directive 2016/1148" means Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union [M7], as amended from time to time;

"Drinking Water Quality Regulator for Scotland" means the person appointed by the Scottish Ministers under section 7(1) of the Water Industry (Scotland) Act 2002 **M8**;

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

[[F2]"First-tier Tribunal" has the meaning given by section 3(1) of the Tribunals, Courts and Enforcement Act 2007**]**;

"GCHQ" means the Government Communications Headquarters within the meaning of section 3 of the Intelligence Services Act 1994 **M9**;

"incident" means any event having, or capable of having, an ~~an actual~~ adverse effect on the operation or security of network and information systems; *[(15) Reporting of incidents by regulated persons]*

"managed service" has the meaning given to it in (3B) *[(9) Managed Service Providers]*

"network and information system" ("NIS") means—

(a) an electronic communications network within the meaning of section 32(1) of the Communications Act 2003 **M10**;

(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;

[[F2]"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) **[**[F3]or (2A)**]** or is designated as an operator of an essential service under regulation 8(3);**]**

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

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

F4

"relevant digital service" means an online marketplace, an online search engine or a cloud computing service; *[(7) Digital Services]*

"relevant law-enforcement authority" has the meaning given in section 63A(1A) of the Police and Criminal Evidence Act 1984 [M11]; and

[[F5]"representative" means any natural or legal person established in the United Kingdom who is able to act on behalf of an RDSP ~~digital service provider~~ established outside the United Kingdom with regard to its obligations under these Regulations; and**]** *[(7) Digital Services]*

"risk" means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems.

(2A) For the purposes of the definition of "cloud computing service" in paragraph (2) –

(a) "broad remote access" means the ability to access and use the service from any authorised location or facility, by means of any capable device or platform (including a computer or mobile device);

(b) a pool of shareable computing resources is "scalable and elastic" if it is capable of being automatically increased, or deprovisioned, according to demand. *[(7) Digital Services]*

(3) In these Regulations a reference to—

[[F6](a) an Article, Annex or paragraph of an Article or Annex is a reference to the Article, Annex or paragraph as numbered in Directive 2016/1148.**]**

(b) a numbered regulation, paragraph or Schedule is a reference to the regulation, paragraph or Schedule as numbered in these Regulations;

(c) "the relevant authorities in a Member State" is a reference to the designated single point of contact ("SPOC"), computer security incident response team ("CSIRT") **[**[F7]or**]** national competent authorities for that Member State;

(d) the "designated competent authority for **[**[F8]an OES**]**" is a reference to the competent authority that is designated under regulation 3(1) for the subsector in relation to which **[**[F9]that OES**]** provides an essential service;

(e) a "relevant digital service provider" ("RDSP") is a reference to a person which –

(i) provides a relevant digital service in the United Kingdom (whether or not the person is established in the United Kingdom),

(ii) is not designated under regulation 14H in relation to the provision 15 of that service,

(iii) is not a micro or small enterprise as defined in Commission Recommendation 2003/361/EC, and

(iv) either—

(aa) is not subject to public authority oversight, or

(bb) is subject to public authority oversight but derives more than half of its income from activities of a commercial nature; *[(7) Digital Services]*

(ea) a "relevant managed service provider" ("RMSP") is a reference to a person which -

(i) provides a managed service in the United Kingdom (whether or not the person is established in the United Kingdom),

(ii) is not designated under regulation 14H in relation to the provision of that service,

(iii) is not a micro or small enterprise as defined in Commission Recommendation 2003/361/EC, and

(iv) either—

(aa) is not subject to public authority oversight, or

(bb) is subject to public authority oversight but derives more than half its income from activities of a commercial nature; *[(9) Managed Service Providers]*

(f) the "NIS enforcement authorities" is a reference to the competent authorities designated under regulation 3(1) and the Information Commissioner;

(g) "security of network and information systems" means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

(3A) A person does not provide a relevant digital service by virtue of providing a public electronic communications network or a public electronic communications service (in each case as defined by section 151(1) of the Communications Act 2003). *[7 (Digital Services)]*

(3B) "Managed service" means a service which—

(a) is provided by a person ("P") under a contract entered into by P and another person ("the customer") for the provision of ongoing management of information technology systems for the customer (whether in the form of support and maintenance, monitoring, active administration or other activities), and

~~(a)~~(b) is provided to the customer by means of P, or a person acting on P's behalf, connecting to or otherwise obtaining access to network and information systems relied on by the customer in connection with a business or other activity carried on by the customer. *[(9) Managed Service Providers]*

(3C) For the purposes of paragraph (3B)(b), it does not matter whether the connection or access to the network and information systems in question is established or obtained on the customer's premises or remotely. *[(9) Managed Service Providers]*

(3D) A person does not provide a managed service by virtue of providing -

(a) a data centre service (as defined by paragraph 11(4) of Schedule 2), or

(b) a public electronic communications network or a public electronic communications service (in each case as defined by section 151(1) of the Communications Act 2003).

[(9)Managed Service Providers]

(3E) For the purposes of paragraph (3)(e) and (ea), a person is subject to public authority oversight if the person is subject to the management or control of—

(a) one or more UK public authorities, or

(b) a board more than half of the members of which are appointed by one or more UK public authorities.

In this paragraph, "UK public authority" means a person exercising functions of a public nature in the United Kingdom.

[(11) Digital or managed service providers: meaning of "subject to public authority oversight"]

~~(g)~~

(4) Expressions and words used in these Regulations which are also used in Directive 2016/1148 have the same meaning as in Directive 2016/1148.

(5) Nothing in these Regulations prevents a person from taking an action (or not taking an action) which that person considers is necessary for the purposes of safeguarding the United Kingdom's essential State functions, in particular—

(a) safeguarding national security, including protecting information the disclosure of which the person considers is contrary to the essential interests of the United Kingdom's security; and

(b) maintaining law and order, in particular, to allow for the investigation, detection and prosecution of criminal offences **M13**.

(6) These Regulations apply to—

(a) the United Kingdom, including its internal waters;

(b) the territorial sea adjacent to the United Kingdom;

(c) the sea (including the seabed and subsoil) in any area designated under section 1(7) of the Continental Shelf Act 1964 **M14**.

PART 2

The National Framework

The NIS national strategy

2.—(1) A Minister of the Crown must designate and 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").

(2) 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—

(a) the sectors specified in column 1 of the table in Schedule 1 ("the relevant sectors"); and

(b) digital services.

(3) The NIS national strategy may be published in such form and manner as the Minister considers appropriate.

(4) The NIS national strategy may be reviewed by the Minister at any time and, if it is revised following such a review, the Minister must designate and publish a revised NIS national strategy as soon as reasonably practicable following that review.

(5) The NIS national strategy must, in particular, address the following matters—

(a) the regulatory measures and enforcement framework to secure the objectives and priorities of the strategy;

(b) the roles and responsibilities of the key persons responsible for implementing the strategy;

(c) the measures relating to preparedness, response and recovery, including cooperation between public and private sectors;

(d) education, awareness-raising and training programmes relating to the strategy;

(e) research and development plans relating to the strategy;

(f) a risk assessment plan identifying any risks; and

(g) a list of the persons involved in the implementation of the strategy.

F10(6) .....

(7) Before publishing the NIS national strategy F11..., the Minister may redact any part of it which relates to national security.

(8) In this regulation "a Minister of the Crown" has the same meaning as in section 8(1) of the Ministers of the Crown Act 1975 **M15**.

Designation of national competent authorities

3.—(1) The person specified in column 3 of the table in Schedule 1 is designated as the competent authority, for the territorial jurisdiction indicated in that column, and for the subsector specified in column 2 of that table ("the designated competent authorities").

(2) The Information Commissioner is designated as the competent authority for the United Kingdom for RDSPs and for RMSPs. *[(9) Managed Service Providers]*

(3) In relation to the subsector for which it is designated under paragraph (1), the competent authority must—

(a) review the application of these Regulations;

(b) prepare and publish guidance;

(c) keep a list of all the operators of essential services who are designated, or deemed to be designated, under regulation 8 F12...;

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

(e) send a copy of the lists mentioned in sub-paragraphs (c) and (d) to GCHQ, for the purpose of facilitating the exercise by GCHQ of any of its functions under or by virtue of these Regulations or any other enactment.~~as the SPOC designated under regulation 4, 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 these Regulations, consult and co-operate with— (i) relevant law-enforcement authorities;

F13(ii) .....

(iii) other competent authorities in the United Kingdom;

(iv) the SPOC that is designated under regulation 4; and

(v) the CSIRT that is designated under regulation 5.

(3ZA) Guidance under paragraph (3)(b) must, in particular, include guidance on –

(a) the taking of appropriate and proportionate measures under regulation 10(1) and (2);
(b) the requirements imposed on OESs by regulation 11;
(c) the requirements imposed by regulations 8ZA, 11A and 11C on OESs which provide an essential service of a kind referred to in paragraph 11(2) or (3) of Schedule 2.

(3ZB) When preparing guidance under paragraph (3)(b), a designated competent authority must have regard to any relevant code which is in force, so far as the code appears to the authority to be relevant to persons regulated by it, with a view to ensuring that the guidance is consistent with the code.

(3ZC) When preparing guidance under paragraph (3)(b) that relates to critical suppliers, or to the designation of persons under regulation 14H, a designated competent authority must—

(a) coordinate with other designated competent authorities and the Information Commission with a view to ensuring that, where appropriate, the guidance is consistent with guidance issued or to be issued by those other designated competent authorities and the Information Commission, and

~~(v)~~(b) consult each of the other designated competent authorities and the Information Commission before publishing the guidance. *[(19) Guidance]*

[F14(3A) In relation to the subsector for which it is designated under paragraph (1), the competent authority may consult and co-operate with a public authority in the EU if it is in the interests of effective regulation of that subsector (whether inside or outside the United Kingdom).**]**

(4) In relation to relevant digital services and managed services, the Information Commissioner must— *[(9) Managed Service Providers]*

(a) review the application of these Regulations;

(b) prepare and publish guidance; and

(c) consult and co-operate with the persons mentioned in paragraph (3)(g), in order to fulfil the requirements of these Regulations.

(4A) Guidance under paragraph 4(b) must, in particular, include guidance on –

(a) the taking of appropriate and proportionate measures by RDSPs under regulation 12(1);
(b) the requirements imposed on RDSPs by regulations 12A, 12C and 14;
(c) the taking of appropriate and proportionate measures by RMSPs under regulation 14B(1);
(d) the requirements imposed on RMSPs by regulations 14C, 14E and 14G.

(4B) When preparing guidance under paragraph (4)(b), the Information Commission must have regard to any relevant code which is in force, so far as the code appears to the Information Commission to be relevant to persons regulated by it, with a view to ensuring that the guidance is consistent with the code.

(4C) When preparing guidance under paragraph (4)(b) that relates to critical suppliers, or to the designation of persons under regulation 14H, the Information Commission must—

(a) coordinate with the designated competent authorities with a view to ensuring that, where appropriate, the guidance is consistent with guidance issued or to be issued by those designated competent authorities, and

(b) consult each of the designated competent authorities before publishing the guidance. *[(19) Guidance]*

(5) The guidance that is published [F15]... under paragraph (3)(b) or (4)(b) may be—

(a) published in such form and manner as the competent authority or Information Commissioner considers appropriate; and

(b) reviewed at any time, and if it is revised following such a review, the competent authority or Information Commissioner must publish revised guidance as soon as reasonably practicable.

(5A) A copy of the lists kept by it as required by paragraph (3)(c) and (d) must be sent by a competent authority under paragraph (3)(e)—

(a) before the end of the period of 4 months beginning with the 5 day on which section 18(1) of the Cyber Security and Resilience (Network and Information Systems) Act 2026 comes into force, and

~~(b)~~ (b) subsequently, at annual intervals. *[(18) Sharing and use of information under the NIS Regulations etc.]*

(6) The competent authorities designated under paragraph (1) and the Information Commissioner must have regard to the national strategy that is published under regulation 2(1) when carrying out their duties under these Regulations.

(7) In this regulation, "relevant code" means a code of practice issued under section 36 of the Cyber Security and Resilience (Network and Information Systems) Act 2026. *[(19) Guidance]*

Guidance

3A. - A designated competent authority and the Information Commission must have regard to any relevant guidance published by the Secretary of State when carrying out their functions under these Regulations. *[(19) Guidance]*

Designation of the single point of contact

4.—(1) GCHQ is designated as the SPOC on the security of network and information systems for the United Kingdom.

[[F16](2) The SPOC may liaise with the relevant authorities in any- country or territory outside of the United Kingdom~~Member State of the EU~~, the Cooperation Group and the CSIRTs network if it considers it appropriate.**]** *[(18) Sharing and use of information under the NIS Regulations etc.]*

(2ZA) For the purposes of paragraph (2), an authority in a country or territory outside the United Kingdom is "relevant" if the authority appears to the SPOC to exercise functions which correspond to functions under these Regulations of—

(a) a person designated as a competent authority under regulation 3(1) or (2),
(b) the SPOC, or
(c) the CSIRT. *[(18) Sharing and use of information under the NIS Regulations etc.]*

[[F17](2A) The SPOC must—

(a) consult and co-operate, as it considers appropriate, with relevant law enforcement authorities;

(b) co-operate with the NIS enforcement authorities to enable the enforcement authorities to fulfil their obligations under these Regulations.**]**

(3) The SPOC **[**F18may, if it considers it appropriate to do so**]** submit reports to—

(a) the Cooperation Group based on the incident reports it received under regulation 11(9) and 12(15), including the number of notifications and the nature of notified incidents; and

(b) the Commission identifying the number of operators of essential services for each subsector listed in Schedule 2 F19....

F20(4) .....

F20(5) .....

Designation of computer security incident response team

5.—(1) GCHQ is designated as the CSIRT for the United Kingdom in respect of the relevant sectors and digital services.

(2) The CSIRT must—

(a) monitor incidents in the United Kingdom;

(b) provide early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;

(c) respond to any incident notified to it under regulation 11(5)(b) or regulation 12(8);

(d) provide dynamic risk and incident analysis and situational awareness;

F21(e) .....

(f) establish relationships with the private sector to facilitate co-operation with that sector;

(g) promote the adoption and use of common or standardised practices for—

(i) incident and risk handling procedures, and

(ii) incident, risk and information classification schemes; and

(h) co-operate with NIS enforcement authorities to enable the enforcement authorities to fulfil their obligations under these Regulations.

[F22(3) The CSIRT may co-operate with or participate in international co-operation networks (including the CSIRTs network) if the CSIRT considers it appropriate to do so.**]**

Information sharing – enforcement authorities

6.—(1) The NIS enforcement authorities may disclose to another NIS enforcement authority or to a person within paragraph (2) information obtained in the exercise of its functions - ~~share information with **[**F23each other, relevant law enforcement authorities,**]** the CSIRT, **[**F24and public authorities in the EU**]** if that information sharing is~~

~~**[**F25~~

~~(a) necessary for~~

(a) for the purposes of these Regulations or of facilitating the exercise by a ~~performance of any functions of a~~ NIS enforcement authority of any of its functions under or by virtue of these Regulations or any other enactment (including an enactment comprised in, or in an instrument made under, an Act of the Scottish Parliament),~~;~~

~~(a)~~ national security purposes; or

(b)

(c) In connection with ~~purposes related to~~ the prevention or detection of crime (whether or not in the United Kingdom),~~, the investigation of an offence or the conduct of a prosecution;**]**~~

(d) in connection with the investigation of a criminal offence (whether or not in the United Kingdom), or

(e) for the purposes of criminal proceedings (whether or not in the United Kingdom).

(2) The following persons are within this paragraph –

(a) the Secretary of State;
(b) a relevant law-enforcement authority;
(c) the CSIRT;
(d) a UK public authority which does not fall within any of the sub-paragraphs (a) to (c).

(3) A person within paragraph (2) may disclose to a NIS enforcement authority information obtained in the exercise of the person's functions for any of the purposes mentioned in paragraph (1).

For this purpose, the reference in paragraph (2)(b) to a relevant law-enforcement authority is to be read as a reference to a relevant law-enforcement authority which exercises functions in the United Kingdom.

(4) A disclosure under paragraph (1) or (3) must be limited to information which is relevant and proportionate to the purpose for which the disclosure is being made.

(5) A NIS enforcement authority may disclose to the Secretary of State information obtained in the exercise of its functions if the authority considers that the information—

(a) may be relevant for the purposes of a report under section 40 of the Cyber Security and Resilience (Network and Information Systems) Act 2026 (reports on network and information systems legislation),
(b) may assist the Secretary of State in assessing—
  (i) the security and resilience of network and information systems,
  (ii) the provision and availability of data centre services in the United Kingdom, or
  (iii) any other matter relating to cyber security and resilience, or
(c) may assist the Secretary of State in formulating policy relating to—
  (i) a matter mentioned in sub-paragraph (b), or
  (ii) national security.

(6) The Secretary of State may disclose to a NIS enforcement authority information obtained by the Secretary of State in the exercise of functions under these Regulations if the Secretary of State considers that doing so may assist the Secretary of State—

(a) in preparing a report under section 40 of the Cyber Security and Resilience (Network and Information Systems) Act 2026,

(b) in assessing anything mentioned in paragraph (5)(b), or

(c) in formulating policy relating to anything mentioned in paragraph (5)(c).

(7) A NIS enforcement authority may disclose information obtained by the authority in the exercise of its functions to a relevant overseas authority if—

(a) the disclosure is for a purpose mentioned in paragraph (1), and
(b) the disclosure is limited to information which is relevant and proportionate to the purpose for which the disclosure is being made.

(8) In paragraph (7), a "relevant overseas authority", in relation to a disclosure by a NIS enforcement authority, means a person in any country or territory outside the United Kingdom which appears to the NIS enforcement authority to exercise functions of a public nature which—

(a) correspond to functions under these Regulations of—

(i) a person designated as a competent authority under regulation 3(1) or (2),

(ii) the SPOC, or

(iii) the CSIRT, or

~~(a)~~(b) relate to any of the matters mentioned in paragraph (1)(b) to (e).

(9) In this regulation—

"data centre service" means an essential service of a kind referred to in paragraph 11(2) or (3) of Schedule 2;

"UK public authority" means a person exercising functions of a public nature in the United Kingdom. *[(18) Sharing and use of information under the NIS Regulations etc.]*

~~(i)~~

~~(b) limited to information which is relevant and proportionate to the purpose of the information sharing.~~

~~[F26(1A) Information shared under paragraph (1) may not be further shared by the person with whom it is shared under that paragraph for any purpose other than a purpose mentioned in that paragraph unless otherwise agreed by the NIS enforcement authority.]~~

~~(2) When sharing information with [F27a public authority in the EU] under paragraph (1), the NIS enforcement authorities are not required to share—~~

~~(a) confidential information, or~~

~~(b) information which may prejudice the security or commercial interests of operators of essential services or digital service providers.~~

Onward disclosure and further provision about information sharing

6A. – (1) Information disclosed to a person under regulation 6 ("relevant information") must not be further disclosed except in accordance with paragraph (2) or (4).

(2) Relevant information may be disclosed—

(a) to the Secretary of State if—

(i) the disclosure is for a purpose mentioned in regulation 6(1) and the disclosure is limited to information which is relevant and proportionate to that purpose, or

(ii) the person making the disclosure considers that any of sub-paragraphs (a) to (c) of regulation 6(5) applies in relation to the information;

(b) to any of the persons mentioned in paragraph (3), if the disclosure is for a purpose mentioned in regulation 6(1) and the disclosure is limited to information which is relevant and proportionate to that purpose.

(3) The persons referred to in paragraph (2)(b) are—

(a) a relevant law-enforcement authority;

(b) the CSIRT;

(c) a UK public authority (within the meaning of regulation 6) which does not fall within sub-paragraph (a) or (b).

(4) Relevant information may be disclosed to any person with—

(a) the consent of the person from which the information was obtained, and

(b) where the information relates to an identified or identifiable individual or business, the consent of that individual or business.

(5) The disclosure of information under any provision of regulation 6 or this regulation does not breach—

(a) any obligation of confidence owed by the person making the disclosure, or

(b) any other restriction on the disclosure of information (however imposed).

(6) Nothing in regulation 6 or this regulation authorises a disclosure of information which is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.

(7) Regulation 6 and this regulation do not limit the circumstances in which information may be disclosed apart from those regulations. *[(18) Sharing and use of information under the NIS Regulations etc.]*

Use of information by the Information Commission

6B. The Information Commission may use information obtained by it under or by virtue of these Regulations for the purpose of facilitating the exercise of any of its functions under or by virtue of any other enactment, if it considers that the use of the information for that purpose is necessary and proportionate. *[(18) Sharing and use of information under the NIS Regulations etc.]*

Information sharing – Northern Ireland

7.—(1) In order to facilitate the exercise of the Northern Ireland competent authority's functions under these Regulations—

(a) a Northern Ireland Department may share information with the Northern Ireland competent authority; and

(b) the Northern Ireland competent authority may share information with a Northern Ireland Department.

(1A) The disclosure of information under paragraph (1) does not breach—

(a) any obligation of confidence owed by the person making the disclosure, or
(b) any other restriction on the disclosure of information (however imposed).

(1B) This regulation does not authorise a disclosure of information which is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016. *[(18) Sharing and use of information under the NIS Regulations etc.]*

~~(b)~~

(2) In this regulation—*)*

(a) "the Northern Ireland competent authority" means the competent authority that is specified for Northern Ireland in column 3 of the table in Schedule 1 in relation to the subsectors specified in column 2 of that table; and

(b) "a Northern Ireland Department" means a department mentioned in Schedule 1 to the Departments Act (Northern Ireland) 2016 **M16**.

PART 3

Operators of essential services

Identification of operators of essential services

8.—(1) If a person provides an essential service of a kind referred to in [F28]... 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.

(1ZA) Paragraph (1) applies to a person whether or not the person is established in the United Kingdom. *[(3) Identification of operators of essential services]*

[[F29](1A) Paragraph (1) does not apply to a person in relation to the provision by a person of a public electronic communications network or public electronic communications service (in each case as defined by section 151(1) ~~provider or service provider who is subject to the requirements of sections 105A to 105C~~ of the Communications Act 2003 ~~and in this paragraph "network provider" and "service provider" have the meanings given in section 105A(5) of that Act~~.**]** *[(3) Identification of operators of essential services]*

(2) A person who falls within paragraph (1) must notify the designated competent authority **[**[F30]in writing**]** of that fact before the notification date.

[[F31](2A) Each integrated care board is deemed to be designated as an OES for the healthcare settings subsector and, in relation to an integrated care board, any services provided by it (including the making of arrangements for the provision of services by others) are deemed to be essential services.**]**

(3) Even if a person does not meet the threshold requirement mentioned in paragraph (1)(b), a competent authority may designate that person as an OES for the subsector in relation to which that competent authority is designated under regulation 3(1), if the following conditions are met—

(a) that person provides an essential service of a kind specified in [F32]... Schedule 2 for the subsector in relation to which the competent authority is designated under regulation 3(1);

(b) the provision of that essential service by that person relies on network and information systems; and

(c) the competent authority concludes 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.

(3A) A person may be designated under paragraph (3) whether or not the person is established in the United Kingdom. *[(3) Identification of operators of essential services]*

(4) In order to arrive at the conclusion mentioned in paragraph (3)(c), the competent authority must have regard to the following factors—

(a) the number of users relying on the service provided by the person;

(b) the degree of dependency of the other relevant sectors on the service provided by that person;

(c) 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;

(d) the market share of the essential service provided by that person;

(e) the geographical area that may be affected if an incident impacts on the service provided by that person;

(f) 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;

(g) the likely consequences for national security if an incident impacts on the service provided by that person; and

(h) any other factor the competent authority considers appropriate to have regard to, in order to arrive at a conclusion under this paragraph.

(5) A competent authority must designate an OES under paragraph (3) by notice in writing served on the person who is to be designated and provide reasons for the designation in the notice.

(6) Before a competent authority designates a person as an OES under paragraph (3), the authority may—

F33(a) .....

(b) invite the person to submit any written representations about the proposed decision to designate it as an OES.

F34(7) .....

(7ZA) Subject to paragraph (7ZB), paragraphs (1) and (3) apply in relation to the provision of an essential service of a kind referred to in paragraph 11(2) or (3) of Schedule 2 (a "data centre service") by or on behalf of the Crown.

(7ZB) Paragraphs (1) and (3) do not apply in relation to the provision of a data centre service by or on behalf of the Crown—

(a) where the person providing the service is the Security Service, the Secret Intelligence Service or GCHQ, or

(b) to the extent that the service—

(i) is provided by a person on a commercial basis on behalf of His Majesty's Government, and

(ii) is provided for the purpose of enabling the storage, processing or transmission of information or other material which is classified as "secret" or "top secret" in accordance with the policy of His Majesty's Government on security classification of documents.

[(5) Operators of data centre services: Crown application etc]

[F35(7A) If a person has reasonable grounds to believe that they no longer fall within paragraph (1) or that the conditions for designation under paragraph (3) are no longer met in relation to them, they must as soon as practicable notify the designated competent authority in writing and provide with that notification evidence supporting that belief.

(7B) A competent authority that receives from a person a notification and supporting evidence referred to in paragraph (7A) must have regard to that notification and evidence in considering whether to revoke that person's designation.**]**

(8) A competent authority must maintain a list of all the persons who are deemed to be designated under paragraph (1) **[**F36or (2A)**]** or designated under paragraph (3) for the subsectors in relation to which that competent authority is designated under regulation 3(1).

(9) The competent authority must review the list mentioned in paragraph (8) at regular intervals and in accordance with paragraph (10).

(0) The first review under paragraph (9) must take place before 9th May 2020, and subsequent reviews must take place, at least, biennially.

(1) In this regulation **[**F37the "notification date" means**]**—

(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.

Operators of data centre services: information to be provided in connection with designation

8ZA. —(1) This regulation applies to a person which—

(a) 15 is deemed to be designated under regulation 8(1) as an OES for the data infrastructure subsector in relation to the provision of a data centre service, or
(b) is designated under regulation 8(3) as an OES for the data infrastructure subsector in relation to the provision of a data centre service.

(2) The person must, before the end of the relevant 3-month period, provide the information listed in paragraph (3) to the designated competent authority for the purpose of enabling the authority to maintain the list mentioned in regulation 8(8).

(3) The information is—

(a) the person's name;
(b) the person's proper address;
(c) where the person is a body corporate, the names of the directors of that body;
(d) 30 where the person is a partnership (including a Scottish partnership), the names of the partners or persons having control or management of the partnership business;
(e) up-to-date contact details (including email addresses and telephone numbers).

(4) "The relevant 3-month period" is the period of 3 months beginning with—

(a) where the person is deemed to be designated as mentioned in paragraph (1)(a), the first day on which the person was deemed to be so designated;
(b) where the person is designated as mentioned in paragraph (1)(b), the day on which the notice under regulation 8(5) was served on the person in relation to the designation.

(5) For the purposes of paragraph (3)(b), a person's "proper address" is—

(a) where the person is a body corporate, the address of the registered or principal office of that body;
(b) where the person is a partnership (including a Scottish partnership), the address of the principal office of the partnership;
(c) in any other case, the address where the person will accept service of documents for the purposes of these Regulations.

(6) The person must notify the designated competent authority in writing of any change to the information listed in paragraph (3) as soon as reasonably practicable, and in any event before the end of the period of 7 days beginning with the day on which the change took effect.

(7) In this regulation, "data centre service" means an essential service of a kind referred to in paragraph 11(2) or (3) of Schedule 2. *[(13) Provisions of information by operations of data centre services]*

[F38Nomination by an OES of a person to act on its behalf in the United Kingdom

8A.—(1) This regulation applies to any OES who has their head office outside the United Kingdom and—

(a) provides an essential service of a kind referred to in one or more of paragraphs 1, 2, 3, ~~and~~ 10 and 11 of Schedule 2 (energy, ~~or~~ digital or data infrastructure sector) within the United Kingdom; or *[(13) Provisions of information by operations of data centre services]*

(b) provides an essential service of a kind referred to in one or more of paragraphs 4 to 9 of Schedule 2 (transport, health or drinking water supply and distribution sector) within the United Kingdom and falls within paragraph (2).

(2) An OES falls within this paragraph if they have received a notice in writing from a designated competent authority for the OES requiring them to comply with this regulation.

(3) An OES to whom this regulation applies must—

(a) nominate in writing a person in the United Kingdom with the authority to act on their behalf under these Regulations, including for the service of documents for the purposes of regulation 24 (a "nominated person");

(b) before the relevant date, notify the designated competent authority for the OES in writing of—

(i) their name;

(ii) the name and address of the nominated person; and

(iii) up-to-date contact details of the nominated person (including email addresses and telephone numbers).

(4) The OES must notify the designated competent authority for the OES of any changes to the information notified under paragraph (3)(b) as soon as practicable and in any event within seven days beginning with the day on which the change took effect.

(5) The designated competent authority for the OES and GCHQ may, for the purposes of carrying out their responsibilities under these Regulations, contact the nominated person instead of or in addition to the OES.

(6) A nomination under paragraph (3) is without prejudice to any legal action which could be initiated against the OES.

(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.**]**

Revocation

9.—(1) Even if a person **[**F39is deemed to be designated as an OES under regulation 8(1), the designated competent authority for the OES**]** may revoke the deemed designation **[**F40, by notice in writing**]**, if the authority concludes that an incident affecting the provision of that essential service by that person is not likely to have significant disruptive effects on the provision of the essential service.

(2) **[**F41The designated competent authority for an OES may revoke the designation of that OES**]** under regulation 8(3), by notice **[**F42in writing**]**, if the conditions mentioned in that regulation are no longer met by that person.

(3) Before revoking a deemed designation of a person **[**F43as an OES**]** under regulation 8(1), or a designation of a person **[**F43as an OES**]** under regulation 8(3), the competent authority must—

(a) serve a notice in writing of proposed revocation on that person;

(b) provide reasons for the proposed decision;

(c) invite that person to submit any written representations about the proposed decision within such time period as may be specified by the competent authority; and

(d) consider any representations submitted by the person under sub-paragraph (c) before a final decision is taken to revoke the designation.

(4) In order to arrive at the conclusion mentioned in paragraph (1), the competent authority must have regard to the factors mentioned in regulation 8(4).

F44(5) .....

The security duties of operators of essential services

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

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

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

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

~~**The duty to notify**~~ **Notification of incidents (other than in relation to data centre services)**

11.— (1) This regulation applies to an OES, except so far as it provides an essential service of a kind referred to in paragraph 11(2) or (3) of Schedule 2 (data centre services).

(2) If the OES is aware that an OES incident has occurred or is occurring, it must give the designated competent authority for the OES—

(a) an initial notification containing—
  (i) the OES's name and the essential service to which the incident relates, and
  (ii) brief details of the incident, and
(b) a full notification containing the information listed in paragraph (5) in relation to the incident, so far as known to the OES.

(3) For the purposes of this regulation, an incident is an "OES incident" if—

(a) the incident has affected or is affecting the operation or security of the network and information systems relied on to provide the essential service provided by the OES, and
(b) the impact of the incident in the United Kingdom or any part of it has been, is or is likely to be significant having regard to the factors listed in paragraph (4).

(4) The factors referred to in paragraph (3)(b) are—

(a) the extent of any disruption which has occurred, is occurring or is likely to occur in relation to the provision of the essential service provided by the OES;
(b) the number of users which have been affected, are being affected or are likely to be affected;
(c) the duration of the incident;
(d) the geographical area which has been affected, is being affected or is likely to be affected by the incident;
(e) whether the confidentiality, authenticity, integrity or availability of data relating to users of the essential service has been, is being or is likely to be compromised.

(5) The information referred to in paragraph (2)(b) is—

(a) the OES's name and the essential service to which the incident relates;
(b) the time the incident occurred, its duration and whether it is ongoing;
(c) information concerning the nature of the incident;
(d) where the incident was caused by a separate incident affecting another regulated person, details of that separate incident and of the regulated person in question;
(e) information concerning the impact (including any cross-border impact) which the incident has had, is having or is likely to have (as the case may be);
(f) such other information as the OES considers may assist the designated competent authority in exercising its functions under regulation 11B in relation to the incident.

(6) The notifications required by paragraph (2) must be given—

(a) in the case of an initial notification, before the end of the period of 24 hours beginning with the time at which the OES is first aware that an OES incident has occurred or is occurring;

(b) in the case of a full notification, before the end of the period of 72 hours beginning with that time.

(7) A notification under paragraph (2) must be in writing, and must be provided in such form and manner as the designated competent authority determines.

(8) An OES must send a copy of a notification under paragraph (2) to the CSIRT at the same time as sending the notification to the designated competent authority for the OES.

(9) In this regulation and regulations 11A and 11B, "regulated person" means an OES, an RDSP, an RMSP or a critical supplier.*[(15) Reporting of incidents by regulated persons]*

~~(1) An OES must notify the designated competent authority [F45for the OES in writing] about any incident which has a significant impact on the continuity of the essential service which that OES provides ("a network and information systems ("NIS") incident").~~

~~(2) In order to determine the significance of the impact of an incident an OES must have regard to the following factors—~~

~~(a) the number of users affected by the disruption of the essential service;~~

~~(b) the duration of the incident; and~~

~~(c) the geographical area affected by the incident.~~

~~(3) The notification mentioned in paragraph (1) must—~~

~~(a) provide the following—~~

~~(i) the operator's name and the essential services it provides;~~

~~(ii) the time the NIS incident occurred;~~

~~(iii) the duration of the NIS incident;~~

~~(iv) information concerning the nature and impact of the NIS incident;information concerning any, or any likely, cross-border impact of the NIS incident; and~~

~~(v) any other information that may be helpful to the competent authority; and~~

~~(b) be provided to the competent authority—~~

~~(i) without undue delay and in any event no later than 72 hours after the operator is aware that a NIS incident has occurred; and~~

~~(ii) in such form and manner as the competent authority determines.~~

~~(4) The information to be provided by an OES under paragraph (3)(a) is limited to information which may reasonably be expected to be within the knowledge of that OES.~~

~~(5) After receipt of a notification under paragraph (1), the competent authority must—~~

~~(a) assess what further action, if any, is required in respect of that incident; and~~

~~(b) share the NIS incident information with the CSIRT as soon as reasonably practicable.~~

~~[F46(6) After receipt of the NIS incident information under paragraph (5)(b), and based on that information, the CSIRT may inform the relevant authorities in a Member State if the CSIRT considers that the incident has a significant impact on the continuity of an essential service provision in that Member State.]~~

~~14~~

~~***Changes to legislation:** There are currently no known outstanding effects for the The Network and Information Systems Regulations 2018. (See end of Document for details)*~~

~~(7) After receipt of a notification under paragraph (1), the competent authority or CSIRT may inform—~~

~~(a) the OES who provided the notification about any relevant information that relates to the NIS incident, including how it has been followed up, in order to assist that operator to deal with that incident more effectively or prevent a future incident; and~~

~~(b) the public about the NIS incident, as soon as reasonably practicable, if the competent authority or CSIRT is of the view that public awareness is necessary in order to handle that incident or prevent a future incident.~~

~~(8) Before the competent authority or CSIRT informs the public about a NIS incident under paragraph (7)(b), the competent authority or CSIRT must consult each other and the OES who provided the notification under paragraph (1).~~

~~(9) The competent authority must provide an annual report to the SPOC identifying the number and nature of NIS incidents notified to it under paragraph (1).~~

~~(10) The first report mentioned in paragraph (9) must be submitted on or before 1st July 2018 and subsequent reports must be submitted at annual intervals.~~

~~(11) The CSIRT is not required to share information under paragraph (6) if the information contains—~~

~~(a) confidential information; or~~

~~(b) information which may prejudice the security or commercial interests of an OES.~~

~~(12) Operators of essential services must have regard to any relevant guidance issued by the relevant competent authority when carrying out their duties imposed by paragraphs (1) to (4).~~

Notification of incidents in relation to data centre services

11A.—(1) This regulation applies to an OES so far as it provides an essential service of a kind referred to in paragraph 11(2) or (3) of Schedule 2 (a "data centre service").

(2) If the OES is aware that a data centre incident has occurred or is occurring, it must give the designated competent authority for the OES—

(a) an initial notification containing—

(i) the OES's name and the data centre service to which the incident relates, and

(ii) brief details of the incident, and

(b) a full notification containing the information listed in paragraph (4) in relation to the incident, so far as known to the OES.

(3) In this regulation, "data centre incident" means an incident which could have had, has had, is having or is likely to have—

(a) a significant impact on the operation or security of the network and information systems relied on to provide the data centre service provided by the OES in the United Kingdom,

(b) a significant impact on the continuity of the data centre service provided by the OES in the United Kingdom, or

(c) any other impact, in the United Kingdom or any part of it, which is significant.

(4) The information referred to in paragraph (2)(b) is—

(a) the OES's name and the data centre service to which the incident relates;

(b) the time the incident occurred, its duration and whether it is ongoing;

(c) information concerning the nature of the incident;

(d) where the incident was caused by a separate incident affecting another regulated person, details of that separate incident and of the regulated person in question;

(e) information concerning the impact (including any cross-border impact) which the incident could have had, has had, is having or is likely to have (as the case may be);

(f) such other information as the OES considers may assist the designated competent authority in exercising its functions under regulation 11B in relation to the incident.

(5) The notifications required by paragraph (2) must be given—

(a) in the case of an initial notification, before the end of the period of 24 hours beginning with the time at which the OES is first aware that a data centre incident has occurred or is occurring;

(b) in the case of a full notification, before the end of the period of 72 hours beginning with that time.

(6) A notification under paragraph (2) must be in writing, and must be provided in such form and manner as the designated competent authority determines.

(7) An OES must send a copy of a notification under paragraph (2) to the CSIRT at the same time as sending the notification to the designated competent authority for the OES. *.[(15) Reporting of incidents by regulated persons]*

Functions of designated competent authority and CSIRT in relation to notified incidents

11B.—(1) The CSIRT may, after receiving a copy of a notification under regulation 11 in relation to an incident, notify a relevant authority in a country or territory outside the United Kingdom if the CSIRT considers that—

(a) the incident has had or is likely to have an impact on the operation or security of network and information systems relied on for the provision of an essential service in that country or territory, and

(b) that impact is or is likely to be significant.

(2) The CSIRT may, after receiving a copy of a notification under regulation 11A in relation to an incident, notify a relevant authority in a country or territory outside the United Kingdom if the CSIRT considers that the incident has had or is likely to have a significant impact on—

(a) the operation or security of network and information systems relied on for the provision of a data centre service in that country or territory, or

(b) the continuity of the provision of a data centre service in that country or territory.

(3) For the purposes of paragraphs (1) and (2), an authority in a country or territory outside the United Kingdom is "relevant" if the authority appears to the CSIRT to exercise functions which correspond to functions under these Regulations of—

(a) a person designated as a competent authority under regulation 3(1) or (2),

(b) the SPOC, or

(c) the CSIRT.

(4) A designated competent authority or the CSIRT may, after receiving a notification or a copy of a notification under regulation 11 or 11A in relation to an incident, provide the OES which gave the notification with such information as the authority or the CSIRT (as the case may be) considers may assist the OES to deal with that incident more effectively or prevent a future incident.

(5) Paragraph (6) applies if a designated competent authority or the CSIRT, after consulting the OES which gave the notification under regulation 11 or 11A, is of the view that—

(a) public awareness about the incident to which the notification relates is necessary to manage the incident or prevent a future incident, or

(b) it is otherwise in the public interest for the public to be informed about the incident.

(6) In such a case—

(a) the designated competent authority or the CSIRT may provide the public with such information about the incident as the authority or the CSIRT (as the case may be) considers is necessary for that purpose, or

(b) the designated competent authority may direct the OES which gave the notification to do so.

(7) Before providing information to the public under paragraph (6)(a), the designated competent authority or the CSIRT (as the case may be) must consult—

(a) each other, and

(b) the OES which gave the notification in question.

(8) Before giving a direction under paragraph (6)(b), the designated competent authority must consult the CSIRT and the OES which gave the notification in question.

(9) A designated competent authority or the CSIRT may disclose information from a notification under regulation 11 or 11A in relation to an incident to any regulated person, where the authority or the CSIRT (as the case may be) considers that disclosure is necessary in the interests of preventing other similar incidents.

(10) A disclosure of information under paragraph (1), (2) or (9) or must not contain—

(a) confidential information, or

(b) information which may prejudice the security or commercial interests of a regulated person.

(11) A disclosure of information under or by virtue of paragraph (6) must not contain information which may prejudice the security interests of a regulated person.

(12) Information disclosed to a person under paragraph (9) by a designated competent authority or the CSIRT must not be further disclosed without—

(a) the consent of the designated competent authority or the CSIRT (as the case may be), and

(b) where the information relates to an identified or identifiable regulated person, the consent of that person.

(13) A designated competent authority must provide an annual report to the SPOC, on or before 1 July in each year, identifying the number and nature of incidents notified to it under regulations 11(2)(b) and 11A(2)(b) during the preceding year." *.[(15) Reporting of incidents by regulated persons]*

Incident: notifications of customers

11C.—(1) This regulation applies to an OES so far as it provides an essential service of a kind referred to in paragraph 11(2) or (3) of Schedule 2 (a "data centre service").

(2) After the OES has given a full notification under regulation 11A(2)(b), the OES must, as soon as reasonably practicable—

(a) take reasonable steps to establish which of its customers in the United Kingdom are likely to be adversely affected by the incident to which the notification relates, and

(b) after those steps have been taken, notify those customers of the incident.

(3) When considering whether a customer is likely to be adversely affected by the incident, the OES must take into account—

(a) the extent of any actual or likely disruption to the provision of the data centre service provided by the OES to the customer,

(b) whether the confidentiality, authenticity, integrity or availability of any data relating to the customer is likely to be compromised, and

(c) any other impact on network and information systems of the customer.

(4) A notification under paragraph (2)(b) must—

(a) provide details of the nature of the incident, and

~~(a)~~(b) explain why the OES considers that the customer is likely to be adversely affected by the incident." *[(16) Notification of incidents to customers]*

PART 4

Digital Services

Relevant digital service providers; duties to manage risks to network and information systems. *[(15) Reporting of incidents by regulated persons]*

12.—(1) A RDSP must identify and take appropriate and proportionate measures to manage the risks posed to the security of network and information systems on which it relies to provide, within the **[**F47United Kingdom**]**, the following services—

(a) online marketplace;

(b) online search engine; or

(c) cloud computing service.

(2) The measures taken by a RDSP under paragraph (1) must—

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

(b) prevent and minimise the impact of incidents affecting the security of network and information systems referred to in paragraph (1). ~~their network and information systems with a view to ensuring the continuity of those services; and~~ *[(8) Duties of relevant digital service providers]*

~~(b)~~ (2A) An RDSP must have regard to any relevant guidance issued by the Information Commission when carrying out the duties imposed on it by paragraph (1). *[(8) Duties of relevant digital service providers]*

~~(c) take into account the following elements as specified in Article 2 of EU Regulation 2018/151—~~

~~(i) the security of systems and facilities;~~

~~(ii) incident handling;~~

~~(iii) business continuity management;~~

~~(iv) monitoring auditing and testing; and~~

~~(v) compliance with international standards.~~ *[(8) Duties of relevant digital service providers]*

~~(3) A RDSP must notify the Information Commissioner **[**F48in writing**]** about any incident having a substantial impact on the provision of any of the digital services mentioned in paragraph (1) that it provides.~~

~~(4) The requirement to notify in paragraph (3) applies only if the RDSP has access to information which enables it to assess whether the impact of an incident is substantial.~~

~~(5) The notification mentioned in paragraph (3) must provide the following information—~~

~~**[**F49(a) the RDSP's name and the digital services that it provides;**]**~~

~~(b) the time the F50... incident occurred;~~

~~(c) the duration of the F50... incident;~~

~~(d) information concerning the nature and impact of the F50... incident;~~

~~(e) information concerning any, or any likely, cross-border impact of the F50... incident; and~~

~~(f) any other information that may be helpful to the **[**F51Information Commissioner**]**.~~

~~(6) The notification under paragraph (3) must—~~

~~(a) be made without undue delay and in any event no later than 72 hours after the RDSP is **[**F52first**]** aware that an incident has occurred; and~~

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

(7) In order to determine whether the impact of an incident is substantial the RDSP must—

(a) take into account the following parameters, as specified in Article 3 of EU Regulation 2018/151—

(i) the number of users affected by the incident and, in particular, the users relying on the digital service for the provision of their own services;

(ii) the duration of the incident;

(iii) the geographical area affected by the incident;

(iv) the extent of the disruption to the functioning of the service;

(v) the extent of the impact on economic and societal activities; and **[**[F53](b) have regard to any relevant guidance published by the Information Commissioner.**]**

(8) After receipt of a notification under paragraph (3) the Information Commissioner must share the incident notification with the CSIRT as soon as reasonably practicable.

(9) If an OES is reliant on a RDSP to provide an essential service, the operator must notify the **[**[F54]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 **[**[F55]without undue delay**]**. *[(15) Reporting of incidents by regulated persons]*

[F56](3~~10~~) .....

(11) The Information Commissioner is not required to share information under **[**[F57]these Regulations**]** if the information contains—

(a) confidential information; or

(b) information which may prejudice the security or commercial interests of a RDSP.

(12) If the Information Commissioner or CSIRT—

(a) consults with the RDSP responsible for an incident notification under paragraph (3), and

(b) is of the view that public awareness about that incident is necessary to prevent or manage it, or is in the public interest,

the Information Commissioner or CSIRT may inform the public about that incident or **[**[F58]the Commissioner may**]** direct the RDSP responsible for the notification to do so.

(13) Before the Information Commissioner or CSIRT informs the public about an incident notified under paragraph (3), the Information Commissioner or CSIRT must consult each other and the RDSP who provided the notification.

(14) The Information Commissioner may inform the public about an incident affecting digital services in **[**[F59]a Member State of the EU**]** if—

(a) the relevant authorities in the affected Member State notify the Information Commissioner about the incident;

(b) the Commissioner consults with those relevant authorities; and

(c) the Commissioner is of the view mentioned in **[**[F60]paragraph (12)(b)**]**.

(15) The Information Commissioner must provide an annual report to the SPOC identifying the number and nature of incidents notified to it under paragraph (3).

(16) The first report mentioned in paragraph (15) must be submitted on or before 1st July 2018 and subsequent reports must be submitted at annual intervals after that date. *[(15) Reporting of incidents by regulated persons*

[F61](4~~17~~)

Notification of RDSP incidents

12A. – (1) If an RDSP is aware that an RDSP incident has occurred or is occurring, it must give the Information Commission –

(a) an initial notification containing—
  (i) the RDSP's name and the relevant digital service to which the incident relates, and
  (ii) brief details of the incident, and
(b) a full notification containing the information listed in paragraph (4) in relation to the incident, so far as known to the RDSP.

(2) For the purposes of this regulation, an incident is an "RDSP incident" if—

(a) the incident has affected or is affecting the operation or security of the network and information systems relied on to provide the relevant digital service provided by the RDSP, and
(b) the impact of the incident in the United Kingdom or any part of it has been, is or is likely to be significant having regard to the factors listed in paragraph (3).

(3) The factors referred to in paragraph (2)(b) are—

(i) the extent of any disruption which has occurred, is occurring or is likely to occur in relation to the provision of the relevant digital service provided by the RDSP;
(ii) the number of users which have been affected, are being affected or are likely to be affected;
(iii) the duration of the incident;
(iv) the geographical area which has been affected, is being affected or is likely to be affected by the incident;
(v) whether the confidentiality, authenticity, integrity or availability of data relating to users of the relevant digital service has been, is being or is likely to be compromised;
(vi) whether there has been, is or is likely to be any impact as a result of the incident on network and information systems of users of the service;
(vii) any impact that the incident has had, is having or is likely to have on the economy or the day-to-day functioning of society.

(4) The information referred to in paragraph (1)(b) is—

(a) the RDSP's name and the relevant digital service to which the incident relates;
(b) the time the incident occurred, its duration and whether it is ongoing;
(c) information concerning the nature of the incident;
(d) where the incident was caused by a separate incident affecting another regulated person, details of that separate incident and of the regulated person in question;
(e) information concerning the impact (including any cross-border impact) which the incident has had, is having or is likely to have (as the case may be);
(f) such other information as the RDSP considers may assist the Information Commission in exercising its functions under regulation 12B in relation to the incident.

(5) The notifications required by paragraph (1) must be given—

(a) in the case of an initial notification, before the end of the period of 24 hours beginning with the time at which the RDSP is first aware that an RDSP incident has occurred or is occurring;
(b) in the case of a full notification, before the end of the period of 72 hours beginning with that time.

(6) A notification under paragraph (1) must be in writing, and must be provided in such form and manner as the Information Commission determines.

(7) An RDSP must send a copy of a notification under paragraph (1) to the CSIRT at the same time as sending the notification to the Information Commission.

(8) In this regulation and regulation 12B, "regulated person" means an OES, an RDSP, an RMSP or a critical supplier. *[(15) Reporting of incidents by regulated persons]*

Functions of Information Commission and CSIRT in relation to notified incidents

12B. – (1) The CSIRT may, after receiving a copy of a notification under regulation 12A in relation to an incident, notify a relevant authority in a country or territory outside the United Kingdom if the CSIRT considers that—

(a) the incident has had or is likely to have an impact on the operation or security of network and information systems relied on for the provision of a relevant digital service in that country or territory, and

(b) that impact is or is likely to be significant.

(2) The Information Commission or the CSIRT may, after receiving a notification or a copy of a notification under regulation 12A in relation to an incident, provide the RDSP which gave the notification with such information as the Information Commission or the CSIRT (as the case may be) considers may assist the RDSP to deal with that incident more effectively or prevent a future incident.

(3) Paragraph (4) applies if the Information Commission or the CSIRT, after consulting the RDSP which gave the notification under regulation 12A, is of the view that—

(a) public awareness about the incident to which the notification relates is necessary to manage the incident or prevent a future incident, or

(b) it is otherwise in the public interest for the public to be informed about the incident.

(4) In such a case—

(a) the Information Commission or the CSIRT may provide the public with such information about the incident as the Information Commission or the CSIRT (as the case may be) considers is necessary for that purpose, or

(b) the Information Commission may direct the RDSP which gave the notification to do so.

(5) Before providing information to the public under paragraph (4)(a), the Information Commission or the CSIRT (as the case may be) must consult—

(a) each other, and

(b) the RDSP which gave the notification in question.

(6) Before giving a direction under paragraph (4)(b), the Information Commission must consult the CSIRT and the RDSP which gave the notification in question.

(7) The Information Commission or the CSIRT may disclose information from a notification under regulation 12A in relation to an incident to any regulated person, where the Information Commission or the CSIRT (as the case may be) considers that disclosure is necessary in the interests of preventing other similar incidents.

(8) The Information Commission may provide information to the public about an incident affecting relevant digital services in a country or territory outside the United Kingdom if—

(a) a relevant authority in the country or territory in question notifies the Information Commission about the incident, and

(b) the Information Commission, having consulted that relevant authority, is of the view that public awareness about the incident to which the notification relates is necessary to manage the incident or prevent a future incident or is otherwise in the public interest.

(9) A disclosure of information under paragraph (1) or (7) must not contain—

(a) confidential information, or

(b) information which may prejudice the security or commercial interests of a regulated person.

(10) A disclosure of information under or by virtue of paragraph (4) or (8) must not contain information which may prejudice the security interests of a regulated person.

(11) Information disclosed to a person under paragraph (7) by the Information Commission or the CSIRT must not be further disclosed without—

(a) the consent of the Information Commission or the CSIRT (as the case may be), and
(b) where the information relates to an identified or identifiable regulated person, the consent of that person.

(12) The Information Commission must provide an annual report to the SPOC, on or before 1 July in each year, identifying the number and nature of incidents notified to it under regulation 12A(1)(b) during the preceding year.

(13) For the purposes of this regulation, an authority in a country or territory outside the United Kingdom is "relevant" if the authority appears to the CSIRT or the Information Commission (as the case may be) to exercise functions which correspond to functions under these Regulations of—

(a) 10 a person designated as a competent authority under regulation 3(1) or (2),
(b) the SPOC, or
(c) the CSIRT.

[(15) Reporting of incidents by regulated persons]

Incidents: notification of customers

12C.—(1) After an RDSP has given a full notification under regulation 12A(1)(b), the RDSP must, as soon as reasonably practicable—

(a) take reasonable steps to establish which of its customers in the United Kingdom are likely to be adversely affected by the incident to which the notification relates, and
(b) after those steps have been taken, notify those customers of the incident.

(2) When considering whether a customer is likely to be adversely affected by the incident, the RDSP must take into account—

(a) the extent of any actual or likely disruption to the provision of the relevant digital service provided by the RDSP to the customer,
(b) whether the confidentiality, authenticity, integrity or availability of any data relating to the customer is likely to be compromised, and
(c) any other impact on network and information systems of the customer.

(3) A notification under paragraph (1)(b) must—

(a) provide details of the nature of the incident, and
(b) explain why the RDSP considers that the customer is likely to be adversely affected by the incident. *[(16) Notification of incidents to customers]*

[F62 Co-operation with the European Union 13. The Information Commissioner may give information and assistance to, and otherwise co-operate with, a public authority in the EU if the Information Commissioner considers that to do so would be in the interests of effective supervision of digital service providers (whether inside or outside the United Kingdom), including in the event of an incident notified under regulation 12A~~(3)~~.**]** *[(15) Reporting of incidents by regulated persons]*

Registration with the Information Commissioner

14.—(1) The Information Commissioner must maintain a register of all RDSPs that have been notified to it.

(2) A RDSP must submit the following details to the Information Commissioner before the registration date for the purpose of maintaining the register mentioned in paragraph (1)—

(a) the name of the RDSP;

(b) the RDSP's proper address;

~~the address of its head office, or of its nominated representative; and~~

(ba) where the RDSP is a body corporate, the names of the directors of that body;

(bb) where the RDSP is a partnership (including a Scottish partnership), the names of the partners or persons having control or management of the partnership business;

~~(b)~~ (bc) which relevant digital services the RDSP provides;

(c) up-to-date contact details (including email addresses and telephone numbers).

(2A) For the purposes of paragraph (2)(b), an RDSP's "proper address" is—

(a) where the RDSP is a body corporate, the address of the registered or principal office of that body;

(b) where the RDSP is a partnership (including a Scottish partnership), the address of the principal office of the partnership;

(c) in any other case, the address where the RDSP will accept service of documents for the purposes of these Regulations.

(3) A RDSP must notify the Information Commissioner **[**[F63]in writing**]** about any changes to the details it submitted under paragraph (2) as soon as reasonably practicable, and in any event before the end of the period of 7 days beginning with the day on which the change took effect. ~~as soon as possible, and in any event within three months of the date on which the change took effect.~~

(4) In this regulation, the "registration date" means—

(a) where the conditions mentioned in regulation 1(3)(e) are satisfied in respect of an RDSP on the day on which section 14 of the Cyber Security and Resilience (Network and Information Systems) Act 2026 comes into force, the date on which the period of 3 months beginning with that day ends;

(b) in any other case, the date on which the period of 3 months beginning with the day on which the conditions mentioned in regulation 1(3)(e) are first satisfied in respect of the RDSP ends.

~~(a) 1st November 2018, in the case of a RDSP who satisfies the conditions mentioned in regulation 1(3)(e) on the coming into force date of these Regulations, or~~

~~(b) in any other case, the date three months after the RDSP satisfies those conditions.~~

(5) The Information Commission must send a copy of the register maintained under paragraph (1) to GCHQ for the purpose of facilitating the exercise by GCHQ of any of its functions under or by virtue of these Regulations or any other enactment—

(a) before the end of the period of 4 months beginning with the day on which section 14 of the Cyber Security and Resilience (Network and Information Systems) Act 2026 comes into force, and

(b) subsequently, at annual intervals. *[(14) Provision of information by providers of digital or managed services etc]*18

[[F64]**Representatives of RDSPs~~digital service providers~~ established outside the United Kingdom**

~~**14A.**—(1) This regulation applies to any digital service provider which—~~

~~(a)~~ This regulation applies to an RDSP which has its principal~~head~~ office outside the United Kingdom., ~~but which offers digital services within the United Kingdom; and~~

~~(b) is not a small or micro enterprise as defined in Commission Recommendation 2003/361/EC.~~

(2) The RDSP ~~digital service provider~~ must—

(a) nominate in writing a representative in the United Kingdom; and

(b) notify the Information Commissioner of the name and contact details of that representative (including an email address and telephone number).

~~(b)~~

(3) The RDSP~~digital service provider~~ must comply with paragraph (2)—

(a) where this regulation applies to the RDSP on the day on which section 14 of the Cyber Security and Resilience (Network and Information Systems) Act 2026 comes into force, before the end of the period of 3 months beginning with that day~~in the case of a provider which is offering digital services within the United Kingdom on the coming into force date of these regulations, within three months of the date on which these regulations come into force~~; or

(b) in any other case, ~~within three months of the provider first offering digital services in the United Kingdom.~~ before the end of the period of 3 months beginning with the day on which the RDSP becomes an RDSP to which this regulation applies (whether for the first time or on a subsequent occasion).

(3A) The RDSP must notify the Information Commission of any change to the information notified under paragraph (2) as soon as reasonably practicable, and in any event before the end of the period of 7 days beginning with—

(a) where the change is to the representative nominated, the day on which the change took effect;

(b) where the change is to the representative's name or contact details, the day on which the RDSP became aware of the change.

~~(b)~~

(4) The Information Commissioner or GCHQ may, for the purposes of carrying out their functions under these Regulations, contact the representative instead of or in addition to the RDSP. ~~digital service provider for the purposes of ensuring compliance with these Regulations~~.

(5) A nomination under paragraph (2~~1~~) is without prejudice to any legal action which could be initiated against the nominating RDSP~~digital service provider~~.**]** *[(14) Provision of information by providers of digital or managed services etc]*

PART 4A

Relevant managed service providers

RMSPs: duties to manage risks to network and information systems

14B.—(1) An RMSP must identify and take appropriate and proportionate measures to manage the risks posed to the security of network and information systems on which it relies for the purpose of providing managed services within the United Kingdom.

(2) The measures taken by an RMSP under paragraph (1) must—

(a) (having regard to the state of the art) ensure a level of security of network and information systems appropriate to the risk posed, and

(b) prevent and minimise the impact of incidents affecting the security of network and information systems referred to in paragraph (1).

(3) An RMSP must have regard to any relevant guidance issued by the Information Commission when carrying out the duties imposed on it by paragraph (1). *[(10) Duties of managed service providers to manage risks]*

Registration of RMSPs with the Information Commission

14C.—(1) The Information Commission must maintain a register of all RMSPs that have been notified to it.

(2) An RMSP must submit the following details to the Information Commission before the registration date for the purpose of enabling the Commission to maintain the register under paragraph (1)—

(a) the name of the RMSP;

(b) the RMSP's proper address;

(c) where the RMSP is a body corporate, the names of the directors of that body;

(d) where the RMSP is a partnership (including a Scottish partnership), the names of the partners or persons having control or management of the partnership business;

(e) up-to-date contact details (including email addresses and telephone numbers).

(3) For the purposes of paragraph (2)(b), an RMSP's "proper address" is—

(a) where the RMSP is a body corporate, the address of the registered or principal office of that body;

(b) where the RMSP is a partnership (including a Scottish partnership), the address of the principal office of the partnership;

(c) in any other case, the address where the RMSP will accept service of documents for the purposes of these Regulations.

(4) "The registration date" means—

(a) where the conditions mentioned in regulation 1(3)(ea) are satisfied in respect of an RMSP on the day on which section 14 of the Cyber Security and Resilience (Network and Information Systems) Act 2026 comes into force, the date on which the period of 3 months beginning with that day ends;

(b) in any other case, the date on which the period of 3 months beginning with the day on which the conditions mentioned in regulation 1(3)(ea) are first satisfied in respect of the RMSP ends.

(5) An RMSP must notify the Information Commission in writing of any change to the information listed in paragraph (2) as soon as reasonably practicable, and in any event before the end of the period of 7 days beginning with the day on which the change took effect.

(6) The Information Commission must send a copy of the register maintained under paragraph (1) to GCHQ for the purpose of facilitating the exercise by GCHQ of any of its functions under or by virtue of these Regulations or any other enactment—

(a) before the end of the period of 4 months beginning with the day on which section 14 of the Cyber Security and Resilience (Network and Information Systems) Act 2026 comes into force, and

~~(a)~~ subsequently, at annual intervals. *[(14) Provision of information by providers of digital or managed services etc]*

Representatives of RMSPs established outside the United Kingdom

14D.—(1) This regulation applies to an RMSP which has its principal office outside the United Kingdom.

(2) The RMSP must—

(a) nominate in writing a representative in the United Kingdom, and

(b) notify the Information Commission of the representative's name and contact details (including an email address and telephone number).

(3) The RMSP must comply with paragraph (2)—

(a) where this regulation applies to the RMSP on the day on which section 14 of the Cyber Security and Resilience (Network and Information Systems) Act 2026 comes into force, before the end of the period of 3 months beginning with that day;

(b) in any other case, before the end of the period of 3 months beginning 1 with the day on which the RMSP becomes an RMSP to which this regulation applies (whether for the first time or on a subsequent occasion).

(4) The RMSP must notify the Information Commission of any change to the information notified under paragraph (2) as soon as reasonably practicable, and in any event before the end of the period of 7 days beginning with—

(a) where the change is to the representative nominated, the day on which the change took effect;

(b) where the change is to the representative's name or contact details, the day on which the RMSP became aware of the change.

(5) The Information Commission or GCHQ may, for the purposes of carrying out their functions under these Regulations, contact the representative instead of or in addition to the RMSP.

(6) A nomination under paragraph (2) is without prejudice to any legal action which could be initiated against the RMSP in question. *[(14) Provision of information by providers of digital or managed services etc]*

Notification of RMSP incidents

14E.—(1) If an RMSP is aware that an RMSP incident has occurred or is occurring, it must give the Information Commission—

(a) an initial notification containing—

(i) the RMSP's name and the managed service to which the incident relates, and

(ii) brief details of the incident, and

(b) a full notification containing the information listed in paragraph (4) in relation to the incident, so far as known to the RMSP.

(2) For the purposes of this regulation, an incident is an "RMSP incident" if—

(a) the incident has affected or is affecting the operation or security of the network and information systems relied on to provide the managed service provided by the RMSP, and

(b) the impact of the incident in the United Kingdom or any part of it has been, is or is likely to be significant having regard to the factors listed in paragraph (3).

(3) The factors referred to in paragraph (2)(b) are—

(a) the extent of any disruption which has occurred, is occurring or is likely to occur in relation to the provision of the managed service provided by the RMSP;

(b) the number of users which have been affected, are being affected or are likely to be affected;

(c) the duration of the incident;

(d) the geographical area which has been affected, is being affected or is likely to be affected by the incident;
(e) whether the confidentiality, authenticity, integrity or availability of data relating to users of the managed service has been, is being or is likely to be compromised;
(f) whether there has been, is or is likely to be any impact as a result of the incident on network and information systems of users of the service;
(g) any impact that the incident has had, is having or is likely to have on the economy or the day-to-day functioning of society.

(4) The information referred to in paragraph (1)(b) is—
(a) the RMSP's name and the managed service to which the incident relates;
(b) the time the incident occurred, its duration and whether it is ongoing;
(c) information concerning the nature of the incident;
(d) where the incident was caused by a separate incident affecting another regulated person, details of that separate incident and of the regulated person in question;
(e) information concerning the impact (including any cross-border impact) which the incident has had, is having or is likely to have (as the case may be);
(f) such other information as the RMSP considers may assist the Information Commission in exercising its functions under regulation 14F in relation to the incident.

(5) The notifications required by paragraph (1) must be given—
(a) in the case of an initial notification, before the end of the period of 24 hours beginning with the time at which the RMSP is first aware that an RMSP incident has occurred or is occurring, and
(b) in the case of a full notification, before the end of the period of 72 hours beginning with that time.

(6) A notification under paragraph (1) must be in writing, and must be provided in such form and manner as the Information Commission determines.

(7) An RMSP must send a copy of a notification under paragraph (1) to the CSIRT at the same time as sending the notification to the Information Commission.

(8) In this regulation and regulation 14F, "regulated person" means an OES, an RDSP, an RMSP or a critical supplier. *[(15) Reporting incidents by regulated persons]*

Functions of Information Commission and CSIRT in relation to notified incidents
14F.—
(1) The CSIRT may, after receiving a copy of a notification under regulation 14E in relation to an incident, notify a relevant authority in a country or territory outside the United Kingdom if the CSIRT considers that—
(a) the incident has had or is likely to have an impact on the operation or security of network and information systems relied on for the provision of a managed service in that country or territory, and
(b) that impact is or is likely to be significant.

(2) The Information Commission or the CSIRT may, after receiving a notification or a copy of a notification under regulation 14E in relation to an incident, provide the RMSP which gave the notification with such information as the Information Commission or the CSIRT (as the case may be) considers may assist the RMSP to deal with that incident more effectively or prevent a future incident.

(3) Paragraph (4) applies if the Information Commission or the CSIRT, after consulting the RMSP which gave the notification under regulation 14E, is of the view that—
(a) public awareness about the incident to which the notification relates is necessary to manage the incident or prevent a future incident, or
(b) it is otherwise in the public interest for the public to be informed about the incident.

(4) In such a case—

(a) the Information Commission or the CSIRT may provide the public with such information as the Information Commission or the CSIRT (as the case may be) considers is necessary for that purpose, or
(b) the Information Commission may direct the RMSP which gave the notification to do so.

(5) Before providing information to the public under paragraph (4)(a), the Information Commission or the CSIRT (as the case may be) must consult—
(a) each other, and
(b) the RMSP which gave the notification in question.

(6) Before giving a direction under paragraph (4)(b), the Information Commission must consult the CSIRT and the RMSP which gave the notification in question.

(7) The Information Commission or the CSIRT may disclose information from a notification under regulation 14E in relation to an incident to any regulated person, where the Information Commission or the CSIRT (as the case may be) considers that disclosure is necessary in the interests of preventing other similar incidents.

(8) The Information Commission may provide information to the public about an incident affecting managed services in a country or territory outside the United Kingdom if—
(a) a relevant authority in the country or territory in question notifies the Information Commission about the incident, and
(b) the Information Commission, having consulted that relevant authority, is of the view that public awareness about the incident to which the notification relates is necessary to manage the incident or prevent a future incident or is otherwise in the public interest.

(9) A disclosure of information under paragraph (1) or (7) must not contain—
(a) confidential information, or
(b) information which may prejudice the security or commercial interests of a regulated person.

(10) A disclosure of information under or by virtue of paragraph (4) or (8) must not contain information which may prejudice the security interests of a regulated person.

(11) Information disclosed to a person under paragraph (7) by the Information Commission or the CSIRT must not be further disclosed without—
(a) the consent of the Information Commission or the CSIRT (as the case may be), and
(b) where the information relates to an identified or identifiable regulated person, the consent of that person.

(12) The Information Commission must provide an annual report to the SPOC, on or before 1 July in each year, identifying the number and nature of incidents notified to it under regulation 14E(1)(b) during the preceding year.

(13) For the purposes of this regulation, an authority in a country or territory outside the United Kingdom is "relevant" if the authority appears to the CSIRT or the Information Commission (as the case may be) to exercise functions which correspond to functions under these Regulations of—
(a) a person designated as a competent authority under regulation 3(1) or (2),
(b) the SPOC, or
(c) the CSIRT. *[(15) Reporting incidents by regulated persons]*

Incidents: notification of customers
14G. –(1) After an RMSP has given a full notification under regulation 14E(1)(b), the RMSP must, as soon as reasonably practicable—
(a) take reasonable steps to establish which of its customers in the United Kingdom are likely to be adversely affected by the incident to which the notification relates, and
(b) after those steps have been taken, notify those customers of the incident.

(2) When considering whether a customer is likely to be adversely affected by the incident, the RMSP must take into account—

(a) the extent of any actual or likely disruption to the provision of the managed service provided by the RMSP to the customer,

(b) whether the confidentiality, authenticity, integrity or availability of any data relating to the customer is likely to be compromised, and

(c) any other impact on network and information systems of the customer.

(3) A notification under paragraph (1)(b) must—

(a) provide details of the nature of the incident, and

~~(a)~~(b) explain why the RMSP considers that the customer is likely to be adversely affected by the incident. *[(16) Notification of incidents to customers]*

Designation of critical suppliers

14H.—(1) A designated competent authority may designate a person ("P") under this regulation if—

(a) P supplies goods or services directly to an OES for which the authority is the designated competent authority,

(b) P relies on network and information systems for the purposes of that supply,

(c) the designated competent authority considers that—

(i) an incident affecting the operation or security of any network and information system relied on by P for the purposes of that supply has the potential to cause disruption to—

(aa) the provision of any essential service by the person to which the supply is made, or

(bb) the provision of essential services, relevant digital services or managed services (whether of a particular kind or generally) by persons to which P supplies goods or services, and

(ii) any such disruption is likely to have a significant impact on the economy or the day-to-day functioning of society in the whole or any part of the United Kingdom, and (d) the designation is not prevented by regulation 14I.

(2) The Information Commission may designate a person ("P") under this regulation if—

(a) P supplies goods or services directly to an RDSP or an RMSP,

(b) P relies on network and information systems for the purposes of that supply,

(c) the Information Commission considers that—

(i) an incident affecting the operation or security of any network and information system relied on by P for the purposes of that supply has the potential to cause disruption to—

(aa) the provision of any relevant digital service or managed service by the person to which the supply is made, or

(bb) the provision of essential services, relevant digital services or managed services (whether of a particular kind or generally) by persons to which P supplies goods or services, and

(ii) any such disruption is likely to have a significant impact on the economy or the day-to-day functioning of society in the whole or any part of the United Kingdom, and

(d) the designation is not prevented by regulation 14I.

(3) In reaching a conclusion for the purposes of paragraph (1)(c)(i) or (2)(c)(i), a designated competent authority or the Information Commission must, in particular, have regard to whether the OES, RDSP or RMSP to which the supply is made by P is likely to be able to obtain the goods or services mentioned in paragraph (1)(a) or (2)(a) (as the case may be) from an alternative source in the event of any such incident.

(4) In reaching a conclusion for the purposes of paragraph (1)(c)(ii) or (2)(c)(ii), a designated competent authority or the Information Commission must, in particular, have regard to the likely nature, scale and duration of the potential disruption to the provision of the service or services (as the case may be).

(5) A person may be designated under this regulation—

(a) by more than one designated competent authority;

(b) by one or more designated competent authorities and the Information Commission.

(6) In considering whether to designate a person ("P") under this regulation, a designated competent authority or the Information Commission must, in particular, consider—

(a) whether the risks that relate to P's supply of goods or services to an OES, an RDSP or an RMSP (as the case may be) could, if the designation were not made, be adequately managed through the duties imposed on that OES, RDSP or RMSP by these Regulations;

(b) whether another person exercises regulatory functions in relation to P (whether or not under these Regulations) and, if so, whether that is likely to be adequate for the management of those risks.

(7) A person may be designated under this regulation whether or not the person is established in the United Kingdom.

(8) In this regulation, references to the supply of goods or services include the supply of goods or services outside the United Kingdom (as well as within it). Restrictions on designation 14I. A person may not be designated under regulation 14H—

(a) in relation to the provision of an essential service for a subsector for which the person is deemed to be designated under regulation 8(1) or (2A) or is designated under regulation 8(3),

(b) in relation to the provision of a relevant digital service by virtue of which the person is an RDSP, or

(c) in relation to the provision of a managed service by virtue of which the person is an RMSP.

[(12) Critical Suppliers]

Restrictions on designation

14I. - A person may not be designated under regulation 14H—

(a) in relation to the provision of an essential service for a subsector for which the person is deemed to be designated under regulation 8(1) or (2A) or is designated under regulation 8(3),

(b) in relation to the provision of a relevant digital service by virtue of which the person is an RDSP, or

(c) in relation to the provision of a managed service by virtue of which the person is an RMSP

[(12) Critical Suppliers]

Designation: consultation and procedure

14J.—(1) Before designating a person ("P") under regulation 14H, a designated competent authority or the Information Commission must—

(a) consult the persons mentioned in paragraph (2) in relation to the proposed designation,

(b) give notice in writing to P which—

(i) provides reasons for the proposed designation, and

(ii) specifies a reasonable period within which P may make written representations about the proposed designation, and

(c) have regard to any representations made to it in accordance with sub-paragraph (b)(ii).

(2) The persons to be consulted under paragraph (1)(a) are—

(a) in the case of a proposed designation by a designated competent authority ("the consulting authority")—

(i) any other designated competent authority which the consulting authority considers has a relevant connection with P, and

(ii) the Information Commission, if the consulting authority considers that the Information Commission has a relevant connection with P,

(b) in the case of a proposed designation by the Information Commission, any designated competent authority which the Information Commission considers has a relevant connection with P, and

(c) in any case, such other persons as the designated competent authority or the Information Commission (as the case may be) considers appropriate.

(3) For the purposes of paragraph (2)(b)—

(a) a designated competent authority has a relevant connection with P if—

(i) P is for the time being designated by that authority under regulation 14H, or

(ii) the authority is the designated competent authority for an OES to which P supplies goods or services directly;

(b) the Information Commission has a relevant connection with P if—

(i) P is for the time being designated by the Information Commission under regulation 14H, or

(ii) P supplies goods or services directly to an RDSP or an RMSP.

(4) Paragraph (5) applies where, after complying with paragraph (1) in relation to a person, a designated competent authority or the Information Commission decides to designate the person under regulation 14H.

(5) The designated competent authority or the Information Commission (as the case may be) must—

(a) give the person a notice confirming the decision, setting out—

(i) the reasons for the decision, and

(ii) the date on which the designation takes effect, and

(b) give a copy of the notice to the persons consulted under paragraph (1)(a).

(6) A designated competent authority or the Information Commission may provide for the date from which a designation under regulation 14H made by it has effect to be a date later than the date set out in the notice under paragraph (5)(a) by giving notice of the new date to all persons to which the original notice was given.

[(12) Critical Suppliers]

Revocation of designation

14K.—(1) Where a designated competent authority has designated a person 1 under regulation 14H, the authority may revoke the designation if it considers that sub-paragraphs (a) to (d) of regulation 14H(1) are not met in relation to the person.

(2) Where the Information Commission has designated a person under regulation 14H, the Information Commission may revoke the designation if it considers that sub-paragraphs (a) to (d) of regulation 14H(2) are not met in relation to the person.

(3) Where a person ("P") for the time being designated under regulation 14H by a designated competent authority has reasonable grounds to believe that if P were not already designated by that authority, the authority would not be able to designate P under regulation 14H, P must, as soon as practicable—

(a) notify the authority of that belief in writing, providing evidence in support of that belief, and

~~(a)~~(b) where P believes that their designation would be prevented by regulation 14I(b) or (c), also notify the Information Commission.

(4) Where a designated competent authority receives a notification and supporting evidence under paragraph (3)(a) from a person, it must have regard to the notification and evidence in considering whether to revoke the person's designation under regulation 14H.

(5) Where a person ("P") for the time being designated under regulation 14H by the Information Commission has reasonable grounds to believe that if P were not already designated by the Information Commission, the Information Commission would not be able to designate P under regulation 14H, P must, as soon as practicable, notify the Information Commission of that belief in writing, providing evidence in support of that belief.

(6) Where the Information Commission receives a notification and supporting evidence under paragraph (5) from a person, it must have regard to the notification and evidence in considering whether to revoke the person's designation under regulation 14H.

(7) Regulation 14J (consultation and procedure) applies in relation to the revocation of a person's designation under this regulation as it applies in relation to the designation of a person under regulation 14H.

[(12) Critical Suppliers]

Co-ordination

14L.—(1) A designated competent authority by which a person ("P") is for the time being designated under regulation 14H must co-ordinate the exercise of its functions under these Regulations in relation to P with—

(a) any other designated competent authority by which P is for the time being designated under regulation 14H, and

(b) the Information Commission, where P is for the time being designated under regulation 14H by the Information Commission.

(2) Where a person ("P") is for the time being designated under regulation 14H by the Information Commission, the Information Commission must co-ordinate the exercise of its functions under these Regulations in relation to P with any designated competent authority by which P is for the time being designated under that regulation.

(3) The relevant regulators must co-ordinate the exercise of their functions under these Regulations so far as those functions relate to determining—

(a) whether a person meets the requirements for designation under regulation 14H, and

(b) where a person meets those requirements—

(i) whether the person should be designated under regulation 14H, and

(ii) if so, by which one or more of the relevant regulators the designation should be made.

(4) For the purposes of paragraph (3)—

(a) a designated competent authority is a relevant regulator in relation to a person if—

(i) the person is for the time being designated by that designated competent authority, or

(ii) it is reasonable to assume that the person may meet the requirements for designation under regulation 14H by that designated competent authority;

(b) the Information Commission is a relevant regulator in relation to a person if—

(i) the person is for the time being designated by the Information Commission, or

(ii) it is reasonable to assume that the person may meet the requirements for designation under regulation 14H by the Information Commission.

(5) In complying with a duty under any of paragraphs (1) to (3), the designated competent authority or the Information Commission (as the case may be) must exercise its power under regulation 15 to request information from any person with which it is required to co-ordinate if the designated competent authority or the Information Commission considers that the person may be expected to have information that is relevant to the duty in question.

(6) A duty imposed by any of paragraphs (1) to (3) does not apply to the extent that compliance with the duty would impose a burden on the designated competent authority or the Information Commission (as the case may be) that is disproportionate to the benefits of compliance.

(7) Nothing in this regulation limits or otherwise affects the application of the consultation and co-operation duties that apply—

(a) to a designated competent authority under regulation 3(3)(g), and

(b) to the Information Commission under regulation 3(4)(c).

(8) For the purposes of this regulation, a person meets the requirements for designation under regulation 14H if—

(a) sub-paragraphs (a) to (d) of regulation 14H(1) are met in relation to the person, or

(b) sub-paragraphs (a) to (d) of regulation 14H(2) are met in relation to the person.

[(12) Critical Suppliers]

PART 5

Information ~~E~~enforcement and penalties *[(20) Power to require information]*

Information notices

15.—(1) A designated competent authority may require a person to which paragraph (3) applies to give the authority such information or documents as it reasonably requires for the purpose of exercising or deciding whether to exercise any of its functions under these Regulations.

(2) The Information Commission may require a person to which paragraph (3) applies to give the Information Commission such information or documents as it reasonably requires for the purpose of exercising or deciding whether to exercise any of its functions under these Regulations.

(3) This paragraph applies to—

(a) in a case within paragraph (1)—

(i) a person regulated by the designated competent authority, and

(ii) any other person (other than the SPOC or the CSIRT) which appears to the designated competent authority to be likely to have the information or documents sought;

(b) in a case within paragraph (2)—

(i) a person regulated by the Information Commission, and

(ii) any other person (other than the SPOC or the CSIRT) which appears to the Information Commission to be likely to have the information or documents sought.

(4) The information or documents which may be required by a designated competent authority under paragraph (1) include, in particular, information or documents for any of the following purposes—

(a) establishing whether a person falls within regulation 8(1) or meets the conditions for designation by the authority under regulation 8(3);

(b) establishing whether a person meets the requirements for designation under regulation 14H by the authority;

(c) deciding whether to designate a person under regulation 8(3) or 14H;

(d) deciding whether to revoke a person's designation under regulation 9 or 14K;

(e) determining the amount of a penalty payable by a person to the authority under regulation 18;

(f) determining the amount of a charge payable by a person under a scheme made by the authority under regulation 20A(1).

(5) The information or documents which may be required by the Information Commission under paragraph (2) include, in particular, information or documents for any of the following purposes—

(a) establishing whether a person is an RDSP or an RMSP;

(b) establishing whether a person meets the requirements for designation under regulation 14H by the Information Commission;

(c) deciding whether to designate a person under regulation 14H;

(d) deciding whether to revoke a person's designation under regulation 14K;

(e) determining the amount of a penalty payable by a person to the Information Commission under regulation 18;

(f) determining the amount of a charge payable by a person under a scheme made by the Information Commission under regulation 20A(1).

(6) The power conferred by paragraph (1) or (2) is to be exercised by giving the person in question a notice in writing (an "information notice") which must—

(a) specify or describe the information or documents sought,

(b) explain why the information or documents are being sought,

(c) specify the manner and form in which the information or documents must be given,

(d) specify the time by which, or period within which, the information or documents must be given, and

(e) include information about the possible consequences of not complying with the notice.

(7) An information notice given to a person to which paragraph (3)(a)(ii) or (b)(ii) applies—

(a) may take the form of a general request for a category of persons specified in the notice to provide the information or documents specified or described in the notice;

(b) may be given by being published in such manner as the person giving the notice considers appropriate for the purpose of bringing the notice to the attention of persons described in it as persons from which the information or documents are required.

(8) A person to which an information notice is given under this regulation must comply with the requirements imposed by the notice.

(9) For the purposes of this regulation—

(a) a person is regulated by a designated competent authority if the person is—

(i) an OES within a subsector specified in column 2 of the table in Schedule 1 for which the authority is specified in column 3 of that table, or

(ii) a person designated by the authority under regulation 14H (critical suppliers);

(b) a person is regulated by the Information Commission if the person is—

(i) an RDSP or an RMSP, or

(ii) a person designated by the Information Commission under regulation 14H (critical suppliers). *[(20) Powers to require information]*

~~In order to assess whether a person should be an OES, a designated competent authority may serve an information notice [F65in writing] upon any person requiring that person to provide it with [F66all such information as] it reasonably requires to establish whether—~~

~~(a) a threshold requirement described in F67... Schedule 2 is met; or~~

~~(b) the conditions mentioned in regulation 8(3) are met.~~

~~(2) A designated competent authority may serve an information notice [F68in writing] upon an OES requiring [F69the OES] to provide it with [F70all such information as] it reasonably requires [F71for one or more of the following purposes]—~~

~~[F72(a) to assess the security of the OES's network and information systems;~~

~~(b) to establish whether there have been any events that the authority has 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;~~

~~(c) to identify any failure of the OES to comply with any duty set out in these Regulations;~~

~~(d) to 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.]~~

(3) The Information Commissioner may serve upon a RDSP an information notice [F73in writing] requiring that RDSP to provide the Information Commissioner with [F74all such information as] the Information Commissioner reasonably requires [F75for one or more of the following purposes] —

[F76(a) to assess the security of the RDSP's network and information systems;

(b) to establish whether there have been any events that the Commissioner has 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;

(c) to identify any failure of the RDSP to comply with any duty set out in these Regulations;

(d) to assess the implementation of the RDSP's security policies, including from the results of any inspection conducted under regulation 16 and any underlying evidence in relation to such an inspection.]

F77(4) .....

(5) An information notice must —

(a) describe the information that is required by the designated competent authority or the Information Commissioner;

(b) provide the reasons for requesting such information;

(c) specify the form and manner in which the requested information is to be provided; and

(d) specify the time period within which the information must be provided.

[F78(5A) A person upon whom an information notice has been served under this regulation must comply with the requirements of the notice.]

(6) In a case falling within paragraph (1) the information notice may —

(a) be served by publishing it in such manner as the designated competent authority considers 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

(b) take the form of a general request for a certain category of persons to provide the information that is specified in the notice.

(7) A competent authority or the Information Commissioner may withdraw an information notice by written notice to the person on whom it was served.

(8) An information notice under paragraph (1) may not be served upon the SPOC or CSIRT.

Information gathering: further provision

15A.—(1) The power conferred by regulation 15(1) or (2) to require a person ("P") to give information includes power to require P—

(a) to obtain or generate information or documents;
(b) to collect or retain information or documents that P would not otherwise collect or retain for the purpose of giving it under the provision in question.

(2) An information notice under regulation 15 may be given to a person whether or not the person is established in the United Kingdom.

(3) The powers conferred by regulation 15 are exercisable in relation to information or documents whether stored within or outside the United Kingdom.

(4) A person may not be required under regulation 15 to give a privileged communication to a designated competent authority or the Information Commission.

(5) A "privileged communication" is a communication—

(a) between a professional legal adviser and their client,

(b) made in connection with, or in contemplation of, legal proceedings and for the purposes of those proceedings, which in proceedings in the High Court would be protected from disclosure on grounds of legal professional privilege.

(6) In the application of paragraph (5) to Scotland—

(a) the reference to the High Court is to be read as a reference to the Court of Session;
(b) the reference to legal professional privilege is to be read as a reference to the confidentiality of communications.

(7) An information notice given under regulation 15 by a designated competent authority or the Information Commission may be revoked by that authority or the Information Commission (as the case may be)—

(a) where the notice was given as mentioned in regulation 15(7)(b), by publication of a notice in the same manner as that in which the information notice was published;
(b) otherwise, by the giving of a notice to the recipient of the information notice.

[(20) Powers to require information]

Power of inspection

16.—(1) **[**F79The designated competent authority for an OES may—**]**

(a) conduct **[**F80all or any part of**]** an inspection;

(b) appoint a person to conduct **[**F81all or any part of**]** an inspection on its behalf; F82...

(c) direct the OES to appoint a person who is approved by that authority to conduct **[**F83all or any part of**]** an inspection on its behalf,

F84

....

(2) The Information Commissioner may—

(a) conduct **[**F85all or any part of**]** an inspection;

(b) appoint a person to conduct **[**F86all or any part of**]** an inspection on its behalf; F87...

(c) direct that a RDSP appoint a person who is approved by the Information Commissioner to conduct **[**F88all or any part of**]** an inspection on its behalf,

F89

....

(3) For the purposes of carrying out the inspection under paragraph (1) or (2), the OES or RDSP (as the case may be) must—

(a) pay the reasonable costs of the inspection **[**F90if so required by the relevant competent authority or the Information Commissioner**]**;

(b) co-operate with the **[**F91inspector**]**;

(c) provide the inspector with F92... access to their premises **[**F93in accordance with paragraph (5)(a)**]**;

[F94(d) allow the inspector to examine, print, copy or remove any document or information, and examine or remove any material or equipment, in accordance with paragraph (5)(d);**]**

(e) allow the inspector access to any person from whom the inspector seeks relevant information for the purposes of the inspection;

[F95(f) not intentionally obstruct an inspector performing their functions under these Regulations; and

(g) comply with any request made by, or requirement of, an inspector performing their functions under these Regulations.**]**

(4) The **[**[F96]relevant**]** competent authority or Information Commissioner may appoint a person to **[**[F97]conduct all or any part of**]** an inspection under paragraph (1)(b) or (2)(b) on its behalf on such terms and in such a manner as it considers appropriate.

[[F98](5) An inspector may—

(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;

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

(6) The inspector must—

(a) produce proof of the inspector's identity if requested by any person present at the premises; and

(b) take appropriate and proportionate measures to ensure that any material, document, information or equipment removed in accordance with paragraph (5)(d) is kept secure from unauthorised access, interference and physical damage.

(7) Before exercising any power under paragraph (5)(b) to (d) or (g), the inspector—

(a) must take such measures as appear to the inspector appropriate and proportionate to ensure that the ability of the OES or RDSP, as the case may be, to comply with any duty set out in these Regulations will not be affected; and

(b) 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) Where under paragraph (5)(d) an inspector removes any document, material or equipment, the inspector must provide, to the extent practicable, a notice giving—

(a) sufficient particulars of that document, material or equipment for it to be identifiable; and

(b) details of any procedures in relation to the handling or return of the document, material or equipment.

(9) In this regulation—

(a) a reference to 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;

(b) "inspection" means any activity carried out (including any steps mentioned in paragraph (5)) for the purpose of—

(i) verifying compliance with the requirements of these Regulations; or

(ii) assessing or gathering evidence of potential or alleged failures to comply with the requirements of these Regulations,

including any necessary follow-up activity for either purpose;

(c) "inspector" means any person conducting all or any part of an inspection in accordance with paragraph (1) or (2).**]**

Enforcement [F99notices] for breach of duties

17.—(1) **[**F100Subject to paragraph (2A),**]** the designated competent authority for an OES may serve an enforcement notice upon that OES if the F101... authority has reasonable grounds to believe that the OES has failed to—

[F102(za) notify it under regulation 8(2);

(zb) comply with the requirements stipulated in regulation 8A;**]**

(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);

(e) comply with an information notice issued under regulation 15; or

(f) comply with—

(i) a direction given under regulation 16(1)(c), or

(ii) the requirements stipulated in regulation 16(3).

(2) **[**F103Subject to paragraph (2A),**]** the Information Commissioner may serve an enforcement notice upon a RDSP if the Commissioner has reasonable grounds to believe that the RDSP has failed to—

(a) fulfil its duties under regulation 12(1) or (2);

(b) notify an incident under regulation 12(3);

(c) comply with the notification requirements stipulated in regulation 12(5);

(d) comply with a direction made by the Information Commissioner under regulation 12(12);

[F104(da) comply with the requirements stipulated in regulation 14A;**]**

(e) comply with an information notice issued under regulation 15; or

(f) comply with—

(i) a direction given under regulation 16(2)(c), or

(ii) the requirements stipulated in regulation 16(3).

[F105(2A) Before serving an enforcement notice under paragraph (1) or (2), the relevant competent authority or the Information Commissioner must inform the OES or RDSP, in such form and manner as it considers appropriate having regard to the facts and circumstances of the case, of—

(a) the alleged failure; and

(b) how and by when representations may be made in relation to the alleged failure and any related matters.

(2B) When the relevant competent authority or the Information Commissioner informs the OES or RDSP in accordance with paragraph (2A), it may also provide notice of its intention to serve an enforcement notice.

(2) The relevant competent authority or the Information Commissioner may serve an enforcement notice on the OES or RDSP within a reasonable time, irrespective of whether it has provided any notice in accordance with paragraph (2B), having regard to the facts and circumstances of the case, after it has informed the OES or RDSP in accordance with paragraph (2A).

(2C) The relevant competent authority or the Information Commissioner must have regard to any representations made under paragraph (2A)(b).**]**

(3) An enforcement notice that is served under paragraph (1) or (2) must be in writing and must specify the following—

(a) the reasons for serving the notice;

(b) the alleged failure which is the subject of the notice; **[**F106and**]**

(c) what steps, if any, must be taken to rectify the alleged failure and the time period during which such steps must be taken; F107...

F107(d) .....

[F108(3A) An OES or RDSP upon whom an enforcement notice has been served under paragraph (1) or (2) must comply with the requirements, if any, of the notice regardless of whether the OES or RDSP has paid any penalty imposed on it under regulation 18.**]**

(4) If the relevant competent authority or Information Commissioner is satisfied that no further action is required, having considered—

(a) [F109any**]**

representations submitted in accordance with paragraph **[**F110(2A)**]**; or

(b) any steps taken to rectify the alleged failure;

it must inform the OES or the RDSP, as the case may be, in writing, as soon as reasonably practicable.

(5) The OES or RDSP may request reasons for a decision to take no further action under paragraph (4) within 28 days of being informed of that decision.

(6) Upon receipt of a request under paragraph (5), the relevant competent authority or Information Commissioner must provide written reasons for a decision under paragraph (4) within a reasonable time and in any event no later than 28 days.

Penalties

18.—**[**F111(1) The designated competent authority for an OES may serve a notice of intention to impose a penalty on the OES if it has 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 considers that a penalty is warranted having regard to the facts and circumstances of the case.

(2) The Information Commissioner may serve a notice of intention to impose a penalty on a RDSP if it has reasonable grounds to believe that the RDSP has failed to comply with a duty referred to in regulation 17(2) or the duty set out in regulation (3A) and considers that a penalty is warranted having regard to the facts and circumstances of the case.**]**

(2A) The Information Commission may serve a notice of intention to impose a penalty on an RMSP if the Information Commission—

(a) has reasonable grounds to believe that the RMSP has failed to comply with a duty referred to in regulation 17(2ZA) or the duty set out in regulation 17(3A), and

(b) considers that a penalty is warranted having regard to the facts and circumstances of the case.

(2B) A designated competent authority or the Information Commission may serve a notice of intention to impose a penalty on a person if the authority or Information Commission (as the case may be)—

(a) has reasonable grounds to believe that the person has failed to comply with—

(i) an information notice given to the person under regulation 15 by the authority or Information Commission (as the case may be), or

(ii) the duty set out in regulation 17(3A), and

~~(2)~~(b) considers that a penalty is warranted having regard to the facts and circumstances of the case.

(3) A **[**F112notice of intention to impose a penalty**]** must be in writing and must specify the following—

(a) the reasons for imposing a penalty;

(b) the sum that is **[**[F113]intended**]** to be imposed as a penalty and how it is to be paid;
(c) the date on which the notice **[**[F114]of intention to impose a penalty**]** is given;

[[F115](d) the period within which a penalty will be required to be paid if a penalty notice is served;

(e) 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

(f) how and when representations may be made about the content of the notice of intention to impose a penalty and any related matters.**]**

[[F116]~~(3A) The relevant competent authority may, after considering any representations submitted in accordance with paragraph (3)(f), serve a penalty notice on the OES with a final penalty decision if the authority is satisfied that a penalty is warranted having regard to the facts and circumstances of the case.~~

~~(3B) The Information Commissioner may, after considering any representations submitted in accordance with paragraph (3)(f), serve a penalty notice on the RDSP with a final penalty decision if the Commissioner is satisfied that a penalty is warranted having regard to the facts and circumstances of the case.~~

(3A) Paragraph (3B) applies where a designated competent authority or the Information Commission has served a notice of intention to impose a penalty on a person.

(3B) The designated competent authority or the Information Commission (as the case may be) may, after considering any representations submitted in accordance with paragraph (3)(f), serve a penalty notice on the person with a final penalty decision if the authority or Information Commission is satisfied that a penalty is warranted having regard to the facts and circumstances of the case.

(3C) The relevant competent authority or the Information Commissioner may serve a notice of intention to impose a penalty or a penalty notice on a person irrespective of whether it has served or is contemporaneously serving an enforcement notice on the person ~~the OES or RDSP~~ under regulation 17~~(1) or (2)~~.

(3D) A penalty notice must—

(a) be given in writing to the person to which it relates~~OES or RDSP~~;

(b) include reasons for the final penalty decision;

(c) require the person to which it relates ~~OES or RDSP~~ to pay—

(i) the penalty specified in the notice of intention to impose a penalty; or

(ii) such penalty as the relevant competent authority or the Information Commissioner considers appropriate in the light of any representations made by the person to which it relates ~~OES or RDSP~~ and any steps taken by the person to which it relates~~OES or RDSP~~ to rectify the failure or to do one or more of the things required by an enforcement notice under regulation 17(3);

(d) specify the period within which the penalty must be paid ("the payment period") and the date on which the payment period is to commence;

(e) provide details of the appeal process under regulation 19A; and

(f) specify the consequences of failing to make payment within the payment period.

(3E) It is the duty of the person served with a penalty notice~~OES or RDSP~~ to comply with any requirement imposed by the~~a penalty~~ notice.**]**

(4) A competent authority or the Information Commissioner may withdraw a penalty notice by informing the person upon whom it was served in writing.

(5) A penalty imposed under this regulation—

(a) must be of an amount which the designated competent authority or the Information Commission (as the case may be) determines is appropriate and proportionate in the circumstances, including having regard to the matters mentioned in paragraph (6);
(b) must not exceed the maximum amount applicable to the failure in respect of which the penalty is imposed.

(6) The matters referred to in paragraph (5)(a) are—

(a) the impact of the failure in respect of which the penalty is imposed,
(b) any steps taken by the person on which the penalty is imposed to remedy the failure or mitigate its impact, and
(c) the person's previous compliance or non-compliance with requirements imposed under or by virtue of these Regulations or regulations under section 29(1) of the Cyber Security and Resilience (Network and Information Systems) Act 2026.

(7) The maximum amount of a penalty that may be imposed on a person is—

(a) in the case of a failure to which paragraph (10) applies, the standard maximum amount;
(b) in the case of a failure to which paragraph (11) applies, the higher maximum amount.

(8) The "standard maximum amount" is—

(a) where the person is an undertaking, the greater of—
(i) £10,000,000, and
(ii) 2% of the turnover of the undertaking (both inside and outside the United Kingdom);
(b) in any other case, £10,000,000.

(9) The "higher maximum amount" is—

(a) where the person is an undertaking, the greater of—
(i) £17,000,000, and
(ii) 4% of the turnover of the undertaking (both inside and outside the United Kingdom);
(b) in any other case, £17,000,000.

(10) This paragraph applies to a failure to comply with a duty referred to in any of the following provisions—

(a) in regulation 17(1) (OES failures)—
(i) sub-paragraph (za) (failure to notify under regulation 8(2));
(ii) sub-paragraph (zaa) (failure to comply with requirements in regulation 8ZA);
(iii) sub-paragraph (zb) (failure to comply with requirements in regulation 8A);
(iv) sub-paragraph (ca) (failure to comply with regulation 11(8));
(v) sub-paragraph (cd) (failure to comply with regulation 11A(7));
(vi) sub-paragraph (cf) (failure to comply with regulation 11B(12), 12B(11) or 14F(11) in relation to the making of a further disclosure);

(b) in regulation 17(2) (RDSP failures)—
(i) sub-paragraph (ca) (failure to comply with regulation 12A(7));
(ii) sub-paragraph (dza) (failure to comply with regulation 11B(12), 12B(11) or 14F(11) in relation to the making of a further disclosure);
(iii) sub-paragraph (dzc) (failure to comply with regulation 14(2) or (3));
(iv) sub-paragraph (da) (failure to comply with requirements in regulation 14A);

(c) in regulation 17(2ZA) (RMSP failures)—
(i) sub-paragraph (b) (failure to comply with regulation 14C(2) or (5));
(ii) sub-paragraph (c) (failure to comply with regulation 14D);
(iii) sub-paragraph (f) (failure to comply with regulation 14E(7));
(iv) sub-paragraph (h) (failure to comply with regulation 11B(12), 12B(11) or 14F(11) in relation to the making of a further disclosure).

(11) This paragraph applies to a failure to comply with a duty referred to in any of the following provisions—

(a) in regulation 17(1) (OES failures)—
(i) sub-paragraph (a) (failure to fulfil the security duties under regulation 10(1) and (2));
(ii) sub-paragraph (b) (failure to notify an incident under regulation 11(2));
(iii) sub-paragraph (c) (failure to comply with regulation 11(6) and (7) in relation to the notification requirements in regulation 11(2));
(iv) sub-paragraph (cb) (failure to give notification in relation to an incident as required by regulation 11A(2));
(v) sub-paragraph (cc) (failure to comply with regulation 11A(5) and (6) in relation to a notification under 11A(2));
(vi) sub-paragraph (ce) (failure to comply with direction under regulation 11B(6)(b));

(vii) sub-paragraph (cg) (failure to comply with regulation 11C(2)(b) and (4));
(viii) sub-paragraph (f) (failure to comply with direction under regulation 16(1)(c) or requirements under regulation 16(3));

(b) in regulation 17(2) (RDSP failures)—

(i) sub-paragraph (a) (failure to fulfil duties under regulation 12(1));
(ii) sub-paragraph (b) (failure to notify an incident under regulation 12A(1));
(iii) sub-paragraph (c) (failure to comply with regulation 12A(5) and (6) in relation to notification requirement under regulation 12A(1));
(iv) sub-paragraph (d) (failure to comply with a direction made by the Information Commission under regulation 12B(4)(b));
~~(i)~~(v) sub-paragraph (dzb) (failure to comply with regulation 12C(1)(b) and (3));
(vi) sub-paragraph (f) (failure to comply with a direction given under regulation 16(2)(c), or the requirements at regulation 16(3));

(c) in regulation 17(2ZA) (RMSP failures)—

(i) sub-paragraph (a) (failure to comply with regulation 14B(1));
(ii) sub-paragraph (d) (failure to give a notification as required by regulation 14E(1));
(iii) sub-paragraph (e) (failure to comply with the requirements in regulation 14E(5) and (6) in relation to a notification under regulation 14E(1));
(iv) sub-paragraph (g) (failure to comply with a direction under regulation 14F(4)(b));
(v) sub-paragraph (i) (failure to comply with regulation 14G(1)(b) and (3));
(vi) sub-paragraph (j) (failure to comply with a direction under regulation 16(2)(c));
(vii) sub-paragraph (k) (failure to comply with regulation 16(3));

(d) regulation 17(2ZB) (failure to comply with information notice).

[(21) Financial Penalties]

~~(5) The sum [F117of any penalty imposed] under this regulation must be an amount that—~~

~~(a) the competent authority or Information Commissioner determines is appropriate and proportionate to the failure in respect of which it is imposed; and~~

~~(b) is in accordance with paragraph (6).~~

~~(6) The amount F118... must—~~

~~(a) not exceed £1,000,000 for any contravention which the [F119NIS] enforcement authority determines [F120was not a material contravention];~~

~~F121(b) .....~~

~~(c) not exceed £8,500,000 for a material contravention which the [F122NIS] enforcement authority determines [F123does not meet the criteria set out in sub-paragraph (d)]; and~~

~~(d) not exceed £17,000,000 for a material contravention which the [F124NIS] enforcement authority determines [F125has or could have created a significant risk to, or significant impact on, or in relation to, the service provision by the OES or RDSP.]~~

~~(7) In this regulation—~~

~~[F126(a)~~

~~"a material contravention" means—~~

~~(i) [F127a 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—~~

~~(aa) sub-paragraphs (a) to (d) of regulation 17(1); or~~

~~(bb) sub-paragraphs (a) to (d) of regulation 17(2); or~~

~~(ii) 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—~~

~~(aa) sub-paragraphs (a) to (d) of regulation 17(1); or~~

~~(bb) sub-paragraphs (a) to (d) of regulation 17(2).]]~~

F128(b) .....

Independent review of designation decisions and penalty decisions

F129**19.**

[130Appeal by an OES or RDSP to the First-tier Tribunal

19A.—(1) An OES may appeal to the First-tier Tribunal against one or more of the following decisions of the designated competent authority for the OES on one or more of the grounds specified in paragraph (3)—

(a) a decision under regulation 8(3) to designate that person as an OES;

(b) a decision under regulation 9(1) or (2) to revoke the designation of that OES;

(c) a decision under regulation 17(1) to serve an enforcement notice on that OES;

(d) a decision under regulation 18(3A) to serve a penalty notice on that OES.

(2) A RDSP may appeal to the First-Tier Tribunal against one or both of the following decisions of the Information Commissioner on one or more of the grounds specified in paragraph (3)—

(a) a decision under regulation 17(2) to serve an enforcement notice on that RDSP;

(b) a decision under regulation 18(3B) to serve a penalty notice on that RDSP.

(3) The grounds of appeal referred to in paragraphs (1) and (2) are—

(a) that the decision was based on a material error as to the facts;

(b) that any of the procedural requirements under these Regulations in relation to the decision have not been complied with and the interests of the OES or RDSP have been substantially prejudiced by the non-compliance;

(c) that the decision was wrong in law;

(d) that there was some other material irrationality, including unreasonableness or lack of proportionality, which has substantially prejudiced the interests of the OES or RDSP.**]**

[F130Decision of the First-tier Tribunal

19B.—(1) The First-tier Tribunal 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.

(2) The Tribunal may, until it has determined the appeal in accordance with paragraph (1) and unless the appeal is withdrawn, suspend the effect of the whole or part of any of the following decisions to which the appeal relates—

(a) a decision under regulation 8(3) to designate a person as an OES;

(b) a decision under regulation 9(1) or (2) to revoke the designation of a person as an OES;

(c) a decision under regulation 17(1) to serve an enforcement notice;

(d) a decision under regulation 17(2) to serve an enforcement notice;

(e) a decision under regulation 18(3A) to serve a penalty notice; or

(f) a decision under regulation 18(3B) to serve a penalty notice.

(3) The Tribunal may—

(a) confirm any decision to which the appeal relates; or

(b) quash the whole or part of any decision to which the appeal relates.

(4) Where the Tribunal quashes the whole or part of a decision to which the appeal relates, it must remit the matter back to the designated competent authority for the OES or, as the case may be, the Information Commissioner, with a direction to that authority or the Commissioner to reconsider the matter and make a new decision having regard to the ruling of the Tribunal.

(5) The relevant competent authority or, as the case may be, the Information Commissioner, must have regard to a direction under paragraph (4).

(6) Where the relevant competent authority or, as the case may be, the Information Commissioner, makes a new decision in accordance with a direction under paragraph (4), that decision is to be considered final.**]**

[F130Enforcement by civil proceedings

A20.—(1) This regulation applies where—

(a) a designated competent authority for an OES has reasonable grounds to believe that the OES has failed to comply with the requirements of an enforcement notice as required by regulation 17(3A); or

(b) the Information Commissioner has reasonable grounds to believe that a RDSP has failed to comply with the requirements of an enforcement notice as required by regulation 17(3A).

(2) This regulation applies irrespective of whether the OES or RDSP has appealed to the First-tier Tribunal under regulation 19A.

(3) But where an OES or RDSP has appealed to the First-tier Tribunal under regulation 19A and the Tribunal has granted a suspension of the effect of the whole or part of the relevant decision under regulation 19B(2), the relevant competent authority or the Information Commissioner, as the case may be, may not bring or continue proceedings under this regulation in respect of that decision or that part of that decision for as long as the suspension has effect.

(4) Where paragraph (1)(a) applies, the relevant competent authority may commence civil proceedings against the OES—

(a) for an injunction to enforce the duty in regulation 17(3A);

(b) for specific performance of a statutory duty under section 45 of the Court of Session Act 1988; or

(c) for any other appropriate remedy or relief.

(5) Where paragraph (1)(b) applies, the Information Commissioner may commence civil proceedings against the RDSP—

(a) for an injunction to enforce the duty in regulation 17(3A);

(b) for specific performance of a statutory duty under section 45 of the Court of Session Act 1988; or

(c) for any other appropriate remedy or relief.

(6) No civil proceedings may be commenced under this regulation before the end of a period of 28 days beginning with the day on which the last relevant enforcement notice was served on the OES or, as the case may be, RDSP.

(7) In this regulation, a reference to civil proceedings is a reference to proceedings, other than proceedings in respect of an offence, before a civil court in the United Kingdom.**]**

Enforcement of penalty notices

20.—(1) This paragraph applies where a sum is payable to an enforcement authority as a penalty under regulation 18.

(2) In England and Wales the penalty is recoverable as if it were payable under an order of the county court or of the High Court.

(3) In Scotland the penalty may be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom.

(4) In Northern Ireland the penalty is recoverable as if it were payable under an order of a county court or of the High Court.

(5) Where action is taken under this paragraph for the recovery of a sum payable as a penalty under regulation 18, the penalty is —

(a) in relation to England and Wales, to be treated for the purposes of section 98 of the Courts Act 2003 M17 (register of judgments and order etc.) as if it were a judgment entered in the county court;

(b) in relation to Northern Ireland, to be treated for the purposes of Article 116 of the Judgments Enforcement (Northern Ireland) Order 1981 [M18] (register of judgments) as if it were a judgment in respect of which an application has been accepted under Article 22 or 23(1) of that Order.

(6) No action may be taken under this paragraph for the recovery of a sum payable as a penalty under regulation 18 if **[**[F131]an appeal has been brought under regulation 19A and the appeal**]** has not been determined or withdrawn.

PART 5A

Powers to impose charges

Periodic charges under charging scheme

20A.—(1) A NIS enforcement authority may impose a charge on a person in respect of the authority's relevant costs if—

(a) a scheme made by the authority for the purposes of this regulation (a "charging scheme") has effect,

(b) the charge relates to a period specified in the charging scheme (a "chargeable period"),

(c) the person is or was regulated by the authority during the whole or part of the chargeable period, and

(d) the charge is imposed in accordance with the charging scheme.

(2) For the purposes of paragraph (1)—

(a) a NIS enforcement authority's "relevant costs" are its costs or expected costs in connection with the exercise of any of its functions under or by virtue of these Regulations or Part 3 or 4 of the Cyber Security and Resilience (Network and Information Systems) Act 2026;

(b) the costs in respect of which a NIS enforcement authority may impose a periodic charge include costs incurred by the authority before the relevant day in preparation for the imposition of charges in accordance with this regulation,

and in sub-paragraph (b) "the relevant day" is the day on which section 17 of the Cyber Security and Resilience (Network and Information Systems) Act 2026 comes into force.

(3) A charging scheme made by a NIS enforcement authority must specify—

(a) the functions of the authority in respect of which a charge is payable in accordance with the scheme,

(b) the chargeable periods under the scheme,

(c) either—

(i) the amount of a charge, or

(ii) how the amount of a charge is to be determined by the authority (including factors to be taken into account in making the determination),

(d) when and how a charge is to be paid, and

(e) the date (not before the end of the 14-day period beginning with the day on which the scheme is published) from which the scheme has effect.

(4) A charging scheme made by a NIS enforcement authority—

(a) may provide for charges to be imposed in respect of anything done by the authority in connection with the enforcement of requirements imposed under or by virtue of these Regulations or Part 3 or 4 of the Cyber Security and Resilience (Network and Information Systems) Act 2026;

(b) may make different provision for different purposes (including different provision in relation to persons of different descriptions or different circumstances);

(c) may provide that a charge is not payable by persons of a description specified in the scheme or if conditions specified in the scheme are met.

(5) A charge payable by a person in accordance with a charging scheme need not relate to the exercise of functions in relation to the person.

(6) A NIS enforcement authority may revise or revoke its charging scheme.

(7) A NIS enforcement authority must publish its charging scheme (including any revised scheme).

(8) Before making or revising a charging scheme, a NIS enforcement authority must consult such of the persons regulated by the authority as it considers appropriate.

(9) No consultation is required under paragraph (8) in relation to revisions of a charging scheme that are only minor.

(10) For the purposes of this regulation, a person ("P") is regulated by a NIS enforcement authority if—

(a) where the NIS enforcement authority is a person designated by regulation 3(1), P is—

(i) an OES within a subsector specified in column 2 of the table in Schedule 1 for which the authority is specified in column 3 of that table, or

(ii) a person in respect of which a designation by the authority under regulation 14H(1) has effect;

(b) where the NIS enforcement authority is the Information Commission, P is—

(i) an RDSP or an RMSP, or

(ii) a person in respect of which a designation by the Information Commission under regulation 14H(1) has effect.

[(17) Power to impose charges]

Further provision about periodic charges under regulation 20A

20B.—(1) Where the amount of a charge payable by a person ("P") to a NIS enforcement authority under regulation 20A is determined by reference to P's turnover in respect of a period specified in the authority's charging scheme, the amount of that turnover is, in the event of a disagreement between P and the authority, the amount determined by the authority.

(2) A charge payable to a NIS enforcement authority in accordance with the authority's charging scheme is recoverable as a civil debt due to the authority.

(3) A NIS enforcement authority must, in relation to each chargeable period in respect of which a charge is payable to the authority under regulation 20A, produce a statement setting out the required information.

(4) The required information is—

(a) the aggregate amount of the charges payable to the authority in relation to the chargeable period which has been received by the NIS enforcement authority,

(b) the aggregate amount of the charges payable to the authority in relation to the chargeable period which remains outstanding and is likely to be paid or recovered, and

(c) the cost to the authority of the exercise of functions in respect of which charges are payable to the authority in relation to the chargeable period.

(5) A NIS enforcement authority must publish a statement produced by it under paragraph (3) in relation to a chargeable period—

(a) if the charges to which the statement relates are payable to the authority before the end of that period, as soon as reasonably practicable after the end of the period;

(b) if the charges to which the statement relates are payable to the authority after the end of that period, as soon as reasonably practicable after the time by which all charges payable to the authority in accordance with its charging scheme are required to be paid.

(6) In this regulation—

"chargeable period", in relation to a charging scheme, means a period specified in the scheme by virtue of regulation 20A(3)(b);

"charging scheme", in relation to a NIS enforcement authority, has the meaning given by regulation 20A(1)(a).

[(17) Power to impose charges]

Charges (other than under periodic charges under regulation 20A)

20C.—(1) A NIS enforcement authority may require a person which is or has been regulated by the authority to pay it a charge in respect of costs incurred by or on behalf of the authority in exercising a function under these Regulations in relation to the person.

(2) Where a person is required by a NIS enforcement authority to pay a charge under paragraph (1), the authority must give the person an invoice stating the costs to which the charge relates.

(3) A NIS enforcement authority may not impose a charge under paragraph (1) in connection with—

(a) costs relating to an appeal under regulation 19A against a decision of the authority,
(b) costs relating to the bringing of proceedings by the authority under regulation A20, or
(c) the exercise of any function in respect of which a charge is payable to the authority in accordance with a scheme made by the authority for the purposes of regulation 20A.

(4) A charge payable under paragraph (1) is recoverable as a civil debt due to the NIS enforcement authority.

(5) The reference in paragraph (1) to a person regulated by a NIS enforcement authority is to be construed in accordance with regulation 20A(10).

[(17) Power to impose charges]

PART 6

Miscellaneous

Fees

21.—(1) A fee is payable by an OES or a RDSP 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 or RDSP.

(2) The fee mentioned in paragraph (1) must be paid to the enforcement authority within 30 days after receipt of the invoice sent by the authority.

(3) 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.

(4) An enforcement authority may determine not to charge a fee under paragraph (1) in any particular case.

(5) A fee payable under this regulation is recoverable as a civil debt.

(6) In this regulation—

(a) 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; and

(b) "enforcement authority" has the same meaning as in regulation 18(7)(b).

Proceeds of penalties

22.—(1) The sum that is received by a NIS enforcement authority as a result of a penalty notice served under regulation 18 must be paid into the Consolidated Fund unless paragraph (2) applies.

(2) The sum that is received as a result of a penalty notice served under regulation 18 by—

(a) the Welsh Ministers must be paid into the Welsh Consolidated Fund established under section 117 of the Government of Wales Act 2006 [M19]; and

(b) the Scottish Ministers or the Drinking Water Quality Regulator for Scotland, must be paid into the Scottish Consolidated Fund established under section 64 of the Scotland Act 1998 [M20]

Enforcement action – general considerations

23.—(1) Before a NIS enforcement authority takes any action under regulation **[**[F132]17(1) or (2), 18(3A) or (3B) or A20,**]** the enforcement authority must consider whether it is reasonable and proportionate, on the facts and circumstances of the case, to take action in relation to the contravention.

(2) The NIS enforcement authority must, in particular, have regard to the following matters—

(a) any representations made by the OES or RDSP, as the case may be, about the contravention and the reasons for it, if any;

(b) any steps taken by the OES or RDSP to comply with the requirements set out in these Regulations;

(c) any steps taken by the OES or RDSP to rectify the contravention;

(d) whether the OES or RDSP had sufficient time to comply with the requirements set out in these Regulations; and

(e) whether the contravention is also liable to enforcement under another enactment.

Service of documents

24.—(1) Any document or notice required or authorised by these Regulations to be served on a person may be served by—

(a) delivering it to that person in person;

(b) leaving it at the person's proper address; or

(c) sending it by post or electronic means to that person's proper address.

(2) In the case of a body corporate, a document may be served on a director of that body.

(3) In the case of a partnership, a document may be served on a partner or person having control or management of the partnership business.

(4) 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.

(5) For the purposes of this regulation "proper address" means—

(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.

(6) In this regulation, "partnership" includes a Scottish partnership.

Review and report

25.—(1) The Secretary of State must—

(a) carry out a review of the regulatory provision contained in these Regulations **1**[F133]and in EU Regulation 2018/151**]**; and

(b) publish a report setting out the conclusions of that review.

(2) The first report must be published on or before 9th May 2020 [1F134], the second report must be published on or before 9th May 2022**]** and subsequent reports must be published at **1**[F135]intervals not exceeding five years**]**.

[F136](3) .....

1[F137](4) Section 30(4) of **1**[F138]the Small Business, Enterprise and Employment Act 2015**]** requires that reports published under this regulation must, in particular—

(a) set out the objectives intended to be achieved by the regulatory provision referred to in paragraph (1)(a);

(b) assess the extent to which those objectives are achieved;

(c) assess whether those objectives remain appropriate; and

(d) if those objectives remain appropriate, assess the extent to which they could be achieved in another way which involves less onerous regulatory provision.**]**

1[F137](5) In this regulation "regulatory provision" has the same meaning as in sections 28 to 32 of that Act.**]**

Department for Digital, Culture, Media and Sport

Matt Hancock
Secretary of State

We consent

Rebecca Harris Paul Maynard
Two of the Lords Commissioners of Her Majesty's Treasury

SCHEDULE 1 Regulation 3

Designated Competent Authorities

Column 1 Relevant sectors	***Column 2 subsectors***	***Column 3 designated competent authorities***
Energy	Electricity	The **[**F139Secretary of State for Energy Security and Net Zero**]** (England and Wales and Scotland) and the Gas and Electricity Markets Authority (acting jointly). The Department of Finance (Northern Ireland)
	Oil	The **[**F139Secretary of State for Energy Security and Net Zero**]** (England and Wales and Scotland) The Department of Finance (Northern Ireland)
	Gas	The **[**F139Secretary of State for Energy Security and Net Zero**]** for the essential services specified in Schedule 2, paragraph 3, sub-paragraphs (5) to (8) (England and Wales and Scotland). Otherwise, the **[**F139Secretary of State for Energy Security and Net Zero**]** and The Gas and Electricity Markets Authority (acting jointly). The Department of Finance (Northern Ireland)
Transport	Air Transport	The Secretary of State for Transport and The Civil Aviation Authority (acting jointly) (United Kingdom).
	Rail Transport	The Secretary of State for Transport (England and Wales and Scotland) The Department of Finance (Northern Ireland)
	Water Transport	The Secretary of State for Transport (United Kingdom)
	Road Transport	The Secretary of State for Transport (England and Wales) The Scottish Ministers (Scotland) The Department of Finance (Northern Ireland)
Health Sector	Health care settings (including hospitals, private clinics and online settings)	The Secretary of State for Health (England) The Welsh Ministers (Wales) The Scottish Ministers (Scotland) The Department of Finance (Northern Ireland)
Drinking water supply and distribution	Drinking water supply and distribution	The Secretary of State for Environment, Food and Rural Affairs (England) The Welsh Ministers (Wales)

		The Drinking Water Quality Regulator for Scotland (Scotland)
		The Department of Finance (Northern Ireland)
Digital Infrastructure	Digital Infrastructure	Office of Communications (United Kingdom)
Data Infrastructure	Data Infrastructure	The Secretary of State for Science, Innovation and Technology and the Office of Communications (acting jointly) (United Kingdom)

[(4) Data centres to be regulated as essential services]

SCHEDULE 2 Regulation 8

Essential Services and Threshold Requirements

The electricity subsector

1.—(1) This paragraph describes the threshold requirements which apply to specified kinds of essential services in the electricity subsector.

(2) For the essential service of electricity supply the threshold requirements are—

(a) in Great Britain—

(i) electricity undertakings that carry out the function of supply to more than 250,000 final customers; or

(ii) electricity undertakings that carry out the function of supply, and generation via generators that when cumulated with the generators operated by affiliated undertakings would have a total capacity, in terms of input to a transmission system, greater than or equal to 2 gigawatts;

(b) in Northern Ireland—

(i) the holder of a supply licence under Article 10(1)(c) of the Electricity (Northern Ireland) Order 1992 M21 who supplies electricity to more than 8,000 consumers; and

(ii) the holder of a generation licence under Article 10(1)(a) of the Electricity (Northern Ireland) Order 1992 with a generating capacity equal to or greater than 350 megawatts.

(3) For the essential service of the single electricity market in Northern Ireland, the threshold requirement is the holder of a Single Electricity Market operator licence under Article 10(1)(d) of the Electricity (Northern Ireland) Order 1992 M22.

(4) For the essential service of electricity transmission, the threshold requirements are—

(a) in Great Britain—

(i) transmission system operators with a potential to disrupt delivery of electricity to more than 250,000 final customers;

(ii) holders of offshore transmission licences where the offshore transmission systems of that licence holder and its affiliated undertakings are directly connected to generators that have a total cumulative capacity, in terms of input to a transmission system, greater than or equal to 2 gigawatts; or

(iii) holders of interconnector licences where the electricity interconnector to which the licence relates has a capacity, in terms of input to a transmission system, greater than or equal to 1 gigawatt;

(b) in Northern Ireland, the holder of a transmission licence under Article 10(1)(b) of the Electricity (Northern Ireland) Order 1992 M23.

(5) For the essential service of electricity distribution, the threshold requirements are—

(a) in Great Britain, distribution system operators with the potential to disrupt delivery of electricity to more than 250,000 final customers;

(b) in Northern Ireland, the holder of a distribution licence under Article 10(1)(bb) of the Electricity (Northern Ireland) Order 1992 M24.

(5A) For the essential service of load control, the threshold requirement in the United Kingdom is a load controller whose potential electrical control, in relation to relevant ESAs managed by the controller, is equal to or greater than 300 megawatts.

(5B) For the purposes of sub-paragraph (5A), a load controller's potential electrical control, in relation to relevant ESAs managed by it, is the aggregate of—

(a) the maximum flow of electricity into all of those relevant ESAs (taken together), and

(b) the maximum flow of electricity out of all of those relevant ESAs (taken together),

which is capable of being achieved in response to load control signals sent by the load controller.

(5C) For the purposes of this paragraph—

(a) "relevant ESA" means an energy smart appliance (as defined by section 238(2) of the Energy Act 2023) which is any of the following—

(i) an electric vehicle;

(ii) a charge point (for electric vehicles);

(iii) an electrical heating appliance;

(iv) a battery energy storage system;

(v) a virtual power plant;

(b) a relevant ESA is "managed" by a person if the person controls the flow of electricity into and out of the relevant ESA by way of load control signals sent by the person to the relevant ESA;

(c) the maximum flow of electricity into or out of a particular relevant ESA is to be determined by reference to the electrical capacity of the relevant ESA as stated by the manufacturer of the relevant ESA.

(5D) Where load control signals are sent to a relevant ESA by a person (an "intermediary") acting under the direction of or on behalf of a load controller, that relevant ESA is to be treated for the purposes of this paragraph as managed by the load controller (and not by the intermediary) unless sub-paragraph (5E) applies.

(5E) Where the intermediary is capable of adjusting or processing the load control signals sent to a relevant ESA, and is authorised by the load controller to do so—

(a) the relevant ESA is to be treated for the purposes of this paragraph as managed by both the load controller and the intermediary, and

(b) the intermediary is also to be treated for those purposes as a load controller

(6) Nuclear electricity generators and generators that are not connected to a transmission system are excluded from the threshold described in sub-paragraph (2)(a)(ii).

(7) Transmission systems for which an offshore transmission licence or interconnector licence applies are excluded from the threshold described in sub-paragraph (4)(a)(i).

(8) In this paragraph—

(a) "affiliated undertaking" has the meaning given by Article 2(12) of Directive 2013/34/EU M25 of the European Parliament and of the Council on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC;

(aa) "charge point" has the same meaning as in Part 2 of the Automated and Electric Vehicles Act 2018 (see section 9 of that Act);

(b) "distribution" has the meaning given by Article 2(5) of Directive 2009/72/EC of the European Parliament and of the Council concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC[M26], ("the Electricity Directive");

(c) "distribution system operator" has the meaning given by Article 2(6) of the Electricity Directive;

(ca) "electric vehicle" means a vehicle which is capable of being propelled by electrical power derived from a storage battery;

(cb) "electrical heating appliance" means any of the following—

(i) a hydronic heat pump;

(ii) a hot water heat pump;

(iii) a hybrid heat pump;

(iv) a direct electric hot water cylinder;

(v) an electric storage heater;

~~(c)~~ (vi) a heat battery;

(d) "electricity undertaking" has the meaning given by Article 2(35) of the Electricity Directive;

(e) "final customer" has the meaning given by Article 2(9) of the Electricity Directive;

(f) "generation" has the meaning given by Article 2(1) of the Electricity Directive and includes the generation of electricity from stored energy, and "generator" must be interpreted accordingly;

(g) "interconnector licence" means a licence granted under section 6(1)(e) of the Electricity Act 1989 M27;

~~(g)~~ (ga) "load control" and "load control signal" have the same meaning as in Part 9 of the Energy Act 2023 (see section 238 of that Act), and "load controller" means a person which provides the service of load control;

(h) "offshore transmission licence" and "offshore transmission" have the meaning given by **[**F140section 6F(8)**]** of the Electricity Act 1989 M28F141...;

(i) "stored energy" means energy that—

(aa) was converted from electricity, and

(bb) is stored for the purpose of its future reconversion into electricity;

(j) "supply" has the meaning given by Article 2(19) of the Electricity Directive;

(k) "transmission" has the meaning given by Article 2(3) of the Electricity Directive; and

(l) "transmission system operator" has the meaning given by Article 2(4) of the Electricity Directive. *[(6) Designation of large load controllers as operators of an essential service]*

The oil subsector

2.—(1) This paragraph describes the threshold requirements which apply to specified kinds of essential services in the oil subsector.

(2) For the essential service of the conveyance of oil through relevant upstream petroleum pipelines, the threshold requirement, in the United Kingdom is the operator of a relevant upstream petroleum pipeline which has a throughput of more than 3,000,000 tonnes of oil equivalent per year excluding natural gas, if that operator does not fall within another threshold requirement in relation to this pipeline under this Schedule.

(3) For the essential service of oil transmission by pipeline, the threshold requirements are—

(a) in Great Britain, operators of any pipeline with throughput F142... of more than 500,000 tonnes of crude oil based fuel per year **[**F143not including transmission of crude oil**]**; and

(b) in Northern Ireland, operators of any pipeline with throughput F144... of more than 50,000 tonnes of crude oil based fuel per year.

(4) For the essential service of the operation of relevant oil processing facilities, the threshold requirement in the United Kingdom is in the case of—

(a) a relevant oil processing facility, **[**F145an operator of a facility with a throughput of more than 3,000,000 tonnes of oil equivalent per year,**]** or

(b) a relevant upstream petroleum pipeline which is connected to and operated from a relevant oil processing facility, **[**F146an operator of a pipeline with a throughput of more than 3,000,000 tonnes of oil equivalent per year.**]**

F147
...

(5) For the essential service of **[**F148crude oil based fuel**]** production, refining, **[**F149onshore**]** storage and transmission the threshold requirements are—

(a) in Great Britain, operators of any facility where that facility has a capacity greater than any of the following values—

(i) storage of 500,000 tonnes of crude oil based fuel;

(ii) production of 500,000 tonnes of crude oil based fuel per year; or

(iii) supply of 500,000 tonnes of crude oil based fuel per year;

(b) in Northern Ireland, the operator of a facility which has a storage capacity of greater than 50,000 tonnes of crude oil based fuel.

(6) For the essential service of the operation of petroleum production projects (other than projects which are primarily used for the storage of gas), the threshold requirement in the United Kingdom is, in the case of—

(i) a relevant offshore installation which is part of a petroleum production project [F150, an operator of an installation with a throughput of more than 3,000,000 tonnes of oil equivalent per year,] or

(ii) a relevant upstream petroleum pipeline which is connected to and operated from such an installation, [F151an operator of a pipeline with a throughput of more than 3,000,000 tonnes of oil equivalent per year]

F152
....

(7) In sub-paragraph (5), the following are included within the description of the essential service—

(a) storage of crude oil based fuel;

(b) production of crude oil based fuels through a range of refining or blending processes, but excluding processes for rendering the oil suitable for transportation; and

(c) supply of crude oil based fuels to retail sites, airports or other users within the United Kingdom.

(8) In this paragraph—

(a) "carbon dioxide pipeline" has the meaning given by section 90(2) of the Energy Act 2011 M29

(b) "crude oil" means any liquid hydrocarbon mixture occurring naturally in the earth whether or not treated to render it suitable for transportation, and includes—

(i) crude oils from which distillate fractions have been removed, and

(ii) crude oils to which distillate fractions have been added;

(c) "crude oil based fuel" means [F153substances derived from crude oil, not including crude oil itself;]

(d) "foreign sector of the continental shelf" has the meaning given by section 90(1) of the Energy Act 2011 M30;

[F154(e) "gas processing facility" has the meaning given by section 12(6) of the Gas Act

(f) 1995;] "gas processing operation" means any of the following operations—

(i) purifying, blending, odorising or compressing gas for the purpose of enabling it to be introduced into a pipeline system operated by a gas transporter or to be conveyed to an electricity generating station, a gas storage facility or any place outside the United Kingdom;

(ii) removing from gas for that purpose any of its constituent gases, or separating from gas for that purpose any oil or water;

(iii) determining the quantity or quality of gas which is or is to be so introduced, or so conveyed, whether generally or by, or on behalf of, a particular person;

(iv) separating, purifying, blending, odorising or compressing gas for the purpose of—

(aa) converting it into a form in which a purchaser is willing to accept delivery from a seller, or

(bb) enabling it to be loaded for conveyance to another place (whether inside or outside the United Kingdom); or

(v) loading gas—

(aa) at a facility which carries out operations of a kind mentioned in paragraph (iv), or

(bb) piped from such a facility

for the purpose of enabling the gas to be conveyed to another place (whether inside or outside the United Kingdom);

(g) "gas transporter" has the meaning given by section 7(1) of the Gas Act 1986 M31;

(h) "oil equivalent" means petroleum and, for the purposes of assessments of throughput, where petroleum is in a gaseous state 1,100 cubic meters of this petroleum at a temperature of 15 degrees Celsius and pressure of one atmosphere is counted as equivalent to one tonne;

(i) "oil processing facility" means any facility which carries out oil processing operations;

(j) "oil processing operations" means any of the following operations—

(i) initial blending and such other treatment of petroleum as may be required to produce stabilised crude oil to the point at which a seller could reasonably make a delivery to a purchaser of such oil;

(ii) receiving stabilised crude oil piped from an oil processing facility carrying out operations of a kind mentioned in sub-paragraph (i), or storing oil so received, prior to their conveyance to another place (whether inside or outside the United Kingdom);

(iii) loading stabilised crude oil piped from a facility carrying out operations of a kind mentioned in sub-paragraph (i) or (ii) for conveyance to another place (whether inside or outside the United Kingdom);

[F155(ja) "operator" means—

(i) in relation to a pipeline—

(aa) the person who is to have or (once any fluid or any mixture of fluids is conveyed) has control over the conveyance of any fluid or any mixture of fluids in the pipeline;

(bb) until that person is known, the person who is to commission or (where commissioning has started) commissions the design and construction of the pipeline; or

(cc) when a pipeline is no longer used or is not for the time being used, the person last having control over the conveyance of fluid or any mixture of fluids in it;

(ii) in relation to a production installation—

(aa) the person appointed by the licensee of the operator or by any other person to manage and control directly the execution of the main functions of a production installation; or

(bb) the licensee, where it is not clear to the designated competent authority that one person has been appointed to perform the functions described in paragraph (aa) or, in the opinion of that authority, the person appointed to perform the functions described in that paragraph is incapable of performing those functions satisfactorily;**]**

(k) "petroleum" has the same meaning as in section 1 of the Petroleum Act 1998 M32, and includes petroleum that has undergone any processing;

(l) "petroleum production project" means a project carried out by virtue of a licence granted under—

(i) section 3 of the Petroleum Act 1998 M33,

(ii) section 2 of the Petroleum (Production) Act 1934 M34, or

(iii) section 2 of the Petroleum (Production) Act (Northern Ireland) 1964

M35, and includes such a project which is used for the storage of gas;

(m) "piped gas" means gas which—

(i) originated from a petroleum production project (or an equivalent project in a foreign sector of the continental shelf), and

(ii) has been conveyed only by means of pipes;

(n) "pipeline" means a pipe or system of pipes for the conveyance of anything;

[F156(na) "production installation" has the meaning given by regulation 2(1) of the Offshore Installations (Safety Case) Regulations 2005;]

(o) "relevant offshore installation" means an offshore installation within the meaning of section 44 of the Petroleum Act 1998 M36 which carries on the activities mentioned in subsection (3)(a) or (c) of that section and is a relevant offshore installation only to the extent it is used to carry on those activities;

(p) "terminal" includes—

(i) facilities for such initial blending and other treatment as may be required to produce stabilised crude oil to the point at which a seller could reasonably make a delivery to a purchaser of such oil;

(ii) oil processing facilities;

(iii) gas processing facilities; and

(iv) a facility for the reception of gas prior to its conveyance to a place outside the United Kingdom;

(q) "upstream petroleum pipeline" means a pipeline or one of a network of pipelines which is—

(i) operated or constructed as part of a petroleum production project (or an equivalent project in a foreign sector of the continental shelf) and is not a carbon dioxide pipeline;

(ii) used to convey petroleum from the site of one or more such projects—

(aa) directly to premises, in order for that petroleum to be used at those premises for power generation or for an industrial process;

(bb) directly to a place outside the United Kingdom;

(cc) directly to a terminal; or

(dd) indirectly to a terminal by way of one or more other terminals, whether or not such intermediate terminals are of the same kind as the final terminal; or

(iii) used to convey gas directly from a terminal to a pipeline system operated by a gas transporter or to any premises.

(9) In sub-paragraph (8)(f), (l), (m), (p) and (q) "gas" means any substance which is or, if it were in a gaseous state, would be gas within the meaning of Part 1 of the Gas Act 1986 M37.

(2) In this paragraph an upstream petroleum pipeline, oil processing facility, or gas processing facility is "relevant" if and in so far as it is situated in—

(a) the United Kingdom;

(b) the territorial sea adjacent to the United Kingdom; or

(c) the sea [F157(including the seabed and subsoil)] in any area designated under section 1(7) of the Continental Shelf Act 1964 M38.

[F158(11) In this paragraph, "Great Britain" includes—

(a) Great Britain;

(b) the territorial sea adjacent to Great Britain; and

(c) the sea (including the seabed and subsoil) in any area designated under section 1(7) of the Continental Shelf Act 1964.]

The gas subsector

3.—(1) This paragraph describes the threshold requirements which apply to specified kinds of essential services in the gas subsector.

(2) For the essential service of gas supply the threshold requirements are—

(a) in Great Britain, supply undertakings that supply gas to more than 250,000 final customers;

(b) in Northern Ireland, the holder of a supply licence under Article 8(1)(c) of the Gas (Northern Ireland) Order 1996 [M39] who supplies gas to more than 2,000 customers.

(3) For the essential service of gas transmission the threshold requirements are—

(a) in Great Britain—

(i) transmission system operators with a potential to disrupt delivery to more than 250,000 final customers; or

(ii) holders of interconnector licences where the gas interconnector to which the licence relates has the technological capacity to input more than 20 million cubic metres of gas per day to a transmission system; and

(b) in Northern Ireland, the holder of a gas conveyance licence under Article 8(1)(a) of the Gas (Northern Ireland) Order 1996.

(4) For the essential service of gas distribution the threshold requirements are—

(a) in Great Britain, distribution system operators with a potential to disrupt delivery to more than 250,000 final customers; and

(b) in Northern Ireland the holder of a licence under Article 8(1)(a) of the Gas (Northern Ireland) Order 1996.

(5) For the essential service of the operation of gas storage facilities, the threshold requirements are—

(a) in Great Britain, storage system operators where the storage facility has the technological capacity to input more than 20 million cubic metres of gas per day to a transmission system; and

(b) in Northern Ireland the holder of a licence under Article 8(1)(b) of the Gas (Northern Ireland) Order 1996 [M40].

(6) For the essential service of the operation of LNG facilities, the threshold requirements are—

(a) in Great Britain, LNG system operators where the LNG facility has the technological capacity to input more than 20 million cubic metres of gas per day to a transmission system; and

(b) in Northern Ireland the holder of a licence under Article 8(1)(d) of the Gas (Northern Ireland) Order 1996 [M41].

(7) For the essential service of the operation of relevant gas processing facilities, the threshold requirement in the United Kingdom is in the case of—

[[F159](a) an operator of a relevant gas processing facility, an operator of a facility with a throughput of more than 3,000,000 tonnes of oil equivalent per year; or

(b) a relevant upstream pipeline and associated infrastructure that is connected to and operated from such a relevant gas processing facility, and critical to the continued operation of that facility, an operator of a pipeline with a throughput of more than 3,000,000 tonnes of oil equivalent per year**]**,

an operator of a facility or pipeline with a throughput of more than 3,000,000 tonnes of oil equivalent per year.

(8) For the essential service of the operation of petroleum production projects (other than projects which are primarily used for the storage of gas), the threshold requirement in the United Kingdom is—

(a) in the case of—

(i) a relevant offshore installation which is part of a petroleum production project (other than a project which is primarily used for the storage of gas), or

(ii) a relevant upstream petroleum pipeline which is connected to and operated from such an installation,

an operator of an installation or pipeline with a throughput of more than 3,000,000 tonnes of oil equivalent per year.

(9) In sub-paragraph (3)(a)(i) the threshold requirement does not include transmission systems for which an interconnector licence applies.

(10) In this paragraph—

(a) "carbon dioxide pipeline" has the meaning given by section 90(2) of the Energy Act 2011 M42

(b) "crude oil" means any liquid hydrocarbon mixture occurring naturally in the earth whether or not treated to render it suitable for transportation, and includes—

(i) crude oils from which distillate fractions have been removed, and

(ii) crude oils to which distillate fractions have been added;

(c) "distribution" has the meaning given by Article 2(5) of Directive 2009/73/EC of the European Parliament and of the Council concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC M43, "the Gas Directive";

(d) "distribution system operator" has the meaning given by Article 2(6) of the Gas Directive;

(e) "final customer" has the meaning given by Article 2(27) of the Gas Directive;

(f) "foreign sector of the continental shelf" has the meaning given by section 90(1) of the Energy Act 2011 M44;

(g) "gas processing facility" means any facility which—

(i) carries out gas processing operations in relation to piped gas;

(ii) is operated otherwise than by a gas transporter; and

(iii) is not an LNG import or export facility (within the meaning of section 12 of the Gas Act 1995 M45);

(h) "gas processing operation" means any of the following operations—

(i) purifying, blending, odorising or compressing gas for the purpose of enabling it to be introduced into a pipeline system operated by a gas transporter or to be conveyed to an electricity generating station, a gas storage facility or any place outside the United Kingdom;

(ii) removing from gas for that purpose any of its constituent gases, or separating from gas for that purpose any oil or water;

(iii) determining the quantity or quality of gas which is or is to be so introduced, or so conveyed, whether generally or by, or on behalf of, a particular person;

(iv) separating, purifying, blending, odorising or compressing gas for the purpose of—

(aa) converting it into a form in which a purchaser is willing to accept delivery from a seller, or

(bb) enabling it to be loaded for conveyance to another place (whether inside or outside the United Kingdom); or

(v) loading gas—

(aa) at a facility which carries out operations of a kind mentioned in paragraph (iv), or

(bb) piped from such a facility,

for the purpose of enabling the gas to be conveyed to another place inside or outside the United Kingdom;

(i) "gas transporter" has the meaning given by section 7(1) of the Gas Act 1986 M46;

(j) "interconnector licence" means a licence granted under section 7ZA of the Gas Act 1986 M47

(k) "LNG facility" has the meaning given by Article 2(11) of the Gas Directive;

(l) "LNG system operator" has the meaning given by Article 2(12) of the Gas Directive;

(m) "oil equivalent" means petroleum and, for the purposes of assessments of throughput, where petroleum is in a gaseous state 1,100 cubic meters of this petroleum at a temperature of 15 degrees Celsius and pressure of one atmosphere is counted as equivalent to one tonne;

(n) "oil processing facility" means any facility which carries out oil processing operations;

(o) "oil processing operations" means any of the following operations—

(i) initial blending and such other treatment of petroleum as may be required to produce stabilised crude oil to the point at which a seller could reasonably make a delivery to a purchaser of such oil;

(ii) receiving stabilised crude oil piped from an oil processing facility carrying out operations of a kind mentioned in sub-paragraph (i), or storing oil so received, prior to their conveyance to another place (whether inside or outside the United Kingdom);

(iii) loading stabilised crude oil piped from a facility carrying out operations of a kind mentioned in sub-paragraph (i) or (ii) for conveyance to another place (whether inside or outside the United Kingdom);

[F160(oa) "operator" means—

(i) in relation to a pipeline—

(aa) the person who is to have or (once any fluid or any mixture of fluids is conveyed) has control over the conveyance of any fluid or any mixture of fluids in the pipeline;

(bb) until that person is known, the person who is to commission or (where commissioning has started) commissions the design and construction of the pipeline; or

(cc) when a pipeline is no longer used or is not for the time being used, the person last having control over the conveyance of fluid or any mixture of fluids in it;

(ii) in relation to a production installation—

(aa) the person appointed by the licensee of the operator or by any other person to manage and control directly the execution of the main functions of a production installation; or

(bb) the licensee, where it is not clear to the designated competent authority that one person has been appointed to perform the functions described in paragraph (aa) or, in the opinion of that authority, the person appointed to perform the functions described in that paragraph is incapable of performing those functions satisfactorily;**]**

(p) "petroleum" has the same meaning as in section 1 of the Petroleum Act 1998 M48, and includes petroleum that has undergone any processing;

(q) "petroleum production project" means a project carried out by virtue of a licence granted under—

(i) section 3 of the Petroleum Act 1998 M49;

(ii) section 2 of the Petroleum (Production) Act 1934 M50; or

(iii) section 2 of the Petroleum (Production) Act (Northern Ireland) 1964 M51; and includes such a project which is used for the storage of gas;

(r) "piped gas" means gas which—

(i) originated from a petroleum production project (or an equivalent project in a foreign sector of the continental shelf); and

(ii) has been conveyed only by means of pipes;

(s) "pipeline" means a pipe or system of pipes for the conveyance of anything;

[F161(sa) "production installation" has the meaning given by regulation 2(1) of the Offshore Installations (Safety Case) Regulations 2005;]

(t) "relevant offshore installation" means an offshore installation within the meaning of section 44 of the Petroleum Act 1998 M52 which carries on the activities mentioned in subsection (3)(a) or (c) of that section and is a relevant offshore installation only to the extent it is used to carry on those activities;

(u) "storage facility" has the meaning given by Article 2(9) of the Gas Directive;

(v) "storage system operator" has the meaning given by Article 2(10) of the Gas Directive;

(w) "supply" has the meaning given by Article 2(7) of the Gas Directive;

(x) "supply undertaking" has the meaning given by Article 2(8) of the Gas Directive;

(y) "terminal" includes—

(i) facilities for such initial blending and other treatment as may be required to produce stabilised crude oil to the point at which a seller could reasonably make a delivery to a purchaser of such oil;

(ii) oil processing facilities;

(iii) gas processing facilities; and

(iv) a facility for the reception of gas prior to its conveyance to a place outside the United Kingdom;

(z) "transmission" has the meaning given by Article 2(3) of the Gas Directive; and

(aa) "transmission system operator" has the meaning given by Article 2(4) of the Gas Directive;

(bb) "upstream petroleum pipeline" means a pipeline or one of a network of pipelines which is—

(i) operated or constructed as part of a petroleum production project (or an equivalent project in a foreign sector of the continental shelf) and is not a carbon dioxide pipeline;

(ii) used to convey petroleum from the site of one or more such projects—

(aa) directly to premises, in order for that petroleum to be used at those premises for power generation or for an industrial process;

(bb) directly to a place outside the United Kingdom;

(cc) directly to a terminal; or

(dd) indirectly to a terminal by way of one or more other terminals, whether or not such intermediate terminals are of the same kind as the final terminal; or

(iii) used to convey gas directly from a terminal to a pipeline system operated by a gas transporter or to any premises.

(11) In—

(a) sub-paragraphs 2(a), 3(a), 4(a), 5(a) and 6(a), or in any provision of the Gas Directive to which these sub-paragraphs cross-refer, any reference to "gas" or "natural gas" means any substance in a gaseous state which consists wholly or mainly of—

(i) methane or hydrogen;

(ii) a mixture of two or more of those gases; or

(iii) a combustible mixture of one or more of those gases and air;

(b) sub-paragraphs 10(h), (q), (r), (y) and (bb), "gas" means any substance which is or, if it were in a gaseous state, would be gas within the meaning of Part 1 of the Gas Act 1986 M53.

(12) In this paragraph an upstream petroleum pipeline, oil processing facility, or gas processing facility is "relevant" if and in so far as it is situated in—

(a) the United Kingdom;

(b) the territorial sea adjacent to the United Kingdom; or

(c) the sea [F162(including the seabed and subsoil)] in any area designated under section 1(7) of the Continental Shelf Act 1964 M54.

[F163(13) In this paragraph, "Great Britain" includes—

(a) Great Britain;

(b) the territorial sea adjacent to Great Britain; and

(c) the sea (including the seabed and subsoil) in any area designated under section 1(7) of the Continental Shelf Act 1964.]

The air transport subsector

4.—(1) This paragraph describes the threshold requirements which apply to specified kinds of essential services in the air transport subsector.

(2) For the essential service of the provision of services by the owner or manager of an aerodrome, the threshold requirement in the United Kingdom is an owner or manager of an aerodrome with annual terminal passenger numbers greater than 10 million.

(3) For the essential service of the provision of air traffic services (as defined in the Transport Act 2000), the threshold requirement in the United Kingdom is—

(a) an entity which is granted a licence by the Secretary of State or the Civil Aviation Authority to provide en-route air traffic services in the United Kingdom; or

(b) an air-traffic service provider at any airport which has annual terminal passenger numbers greater than 10 million.

(4) For the essential service of the provision of services by air carriers, the threshold requirement in the United Kingdom is an air carrier which has—

(a)more than thirty percent of the annual terminal passengers at any United Kingdom airport which has annual terminal passenger numbers greater than 10 million; and

(b) more than 10 million total annual terminal passengers across all United Kingdom airports.

(5) In this paragraph—

(a) "an aerodrome" has the same meaning as in the Civil Aviation Act 1982 M55;

(b) "air carrier" has the same meaning as in Article 3(4) of Regulation (EC) No 300/2008 of the European Parliament and of the Council on common rules in the field of civil aviation security and repealing Regulation EC No 2320/2202 M56.

The water transport subsector

5.—(1) This paragraph describes the threshold requirements which apply to specified kinds of essential services in the water transport subsector.

(2) For the essential service of shipping in the United Kingdom, the threshold requirement is—

(a) a shipping company which handles—

(i) over 5 million tonnes of total annual freight at United Kingdom ports; and

(ii) over thirty percent of the freight at any individual United Kingdom port which fulfils at least one of the following criteria—

(aa) it handles more than fifteen percent of the total roll-on roll-off traffic in the United Kingdom;

(bb) it handles more than fifteen percent of the total lift-on lift-off traffic in the United Kingdom;

(cc) it handles more than ten percent of the total liquid bulk traffic in the United Kingdom; or

(dd) it handles more than twenty percent of the total biomass fuel traffic in the United Kingdom; or

(b) a shipping company with over thirty percent of the annual passenger numbers at any individual United Kingdom port which has annual passenger numbers greater than 10 million.

(3) For the essential service of the provision of services by a harbour authority for a port in the United Kingdom, the threshold requirement is—

(a) a harbour authority for a port which has annual passenger numbers greater than 10 million; or

(b) a harbour authority for a port which fulfils at least one of the following criteria—

(i) it handles more than fifteen percent of the total roll-on roll-off traffic in the United Kingdom;

(ii) it handles more than fifteen percent of the total lift-on lift-off traffic in the United Kingdom;

(iii) it handles more than ten percent of the total liquid bulk traffic in the United Kingdom; or

(iv) it handles more than twenty percent of the total biomass fuel traffic in the United Kingdom.

(4) For the essential service of the provision of services by an operator of a port facility in the United Kingdom, the threshold requirement is—

(a) an operator of a port facility which handles passengers at a port which has annual passenger numbers greater than 10 million; or

(b) an operator of a port facility at a port which fulfils at least one of the following criteria—

(i) it handles more than fifteen percent of the total roll-on roll-off traffic in the United Kingdom;

(ii) it handles more than fifteen percent of the total lift-on lift-off traffic in the United Kingdom;

(iii) it handles more than ten percent of the total liquid bulk traffic in the United Kingdom; or

(iv) it handles more than twenty percent of the total biomass fuel traffic in the United Kingdom;

and where that port facility operator handles the same type of freight for which the port fulfils one of the criteria mentioned in sub-paragraphs (i)-(iv).

(5) For the essential service of vessel traffic services in the United Kingdom, the threshold requirement is—

(a) an operator of vessel traffic services at a port which has annual passenger numbers greater than 10 million; or

(b) an operator of vessel traffic services at a port which fulfils at least one of the following criteria—

(i) it handles more than fifteen percent of the total roll-on roll-off traffic in the United Kingdom;

(ii) it handles more than fifteen percent of the total lift-on lift-off traffic in the United Kingdom;

(iii) it handles more than ten percent of the total liquid bulk traffic in the United Kingdom; or

(iv) it handles more than twenty percent of the total biomass fuel traffic in the United Kingdom.

(6) In this paragraph—

(a) "harbour authority" has the same meaning **[**F164as**]** in section 313(1) of the Merchant Shipping Act 1995 M57;

(b) "port facility" has the same meaning as in regulation 2 of the Port Security Regulations 2009 M58;

(c) "vessel traffic services" has the same meaning as in regulation 2(1) of the Merchant Shipping (Vessel Traffic Monitoring and Reporting Requirements) Regulations 2004 M59.

The rail transport subsector

6.—(1) This paragraph describes the threshold requirements which apply to specified kinds of essential services in the rail transport subsector.

(2) For the essential service of rail services the threshold requirements are—

(a) in Great Britain, any operator of a mainline railway asset but excluding operators of—

(i) railway assets solely for the provision of international rail services;

(ii) railway assets for metro, tram and other light rail, including underground, systems;

(iii) heritage, museum or tourist railways, whether or not they are operating solely on their own network; and

(iv) networks which are privately owned and exist solely for use by the infrastructure owner for its own freight operations or other passenger or freight services for third parties and operators of passenger or freight services on those networks (including high speed rail services);

(b) in Northern Ireland, any railway undertaking in Northern Ireland.

(3) For the essential service of high speed rail services the threshold requirement in the United Kingdom is an operator of a railway asset for high speed rail services.

(4) For the essential service of metros, trams and other light rail services (including underground services), the threshold requirement in the United Kingdom is an operator with more than 50 million annual passenger journeys.

(5) For the essential service of international rail services the threshold requirement in the United Kingdom is an operator of a Channel Tunnel train or the infrastructure manager of the Channel Fixed Link.

(6) In this paragraph—

(a) "operator" and "railway asset" have the same meaning as in section 6 of the Railways Act 1993 M60;

(b) "international rail service" means a rail service where all carriages on the train cross a border of the United Kingdom and that of a Member State, and where the principal purpose of the service is to carry passengers or goods between stations located in the United Kingdom and a station in at least one Member State;

(c) "mainline railway" has the same meaning as in the Railways and Other Guided Transport Systems (Safety) Regulations 2006 M61;

(d) "railway undertaking" has the same meaning as in section 55 of the Transport Act (Northern Ireland) 1967 M62 but excludes heritage railways operating solely on their own network; and

(e) "Channel Tunnel train" has the same meaning as in article 2(1) of the Channel Tunnel (Security) Order 1994 M63 and "Channel Fixed Link" has the same meaning as in section 1 of the Channel Tunnel Act 1987 M64.

The road transport subsector

7.—(1) For the essential service of road transport services, the threshold requirement in the United Kingdom is a road authority responsible for roads in the United Kingdom that have vehicles travelling more than 50 billion miles in total on them.

(2) For the essential service of road services provided by Intelligent Transport Systems, the threshold requirement in the United Kingdom is a road authority that provides Intelligent Transport Systems services which covers roads in the United Kingdom that have vehicles travelling more than 50 billion miles in total on them, per year.

(a) (3) (a) "road authority" has the same meaning **[**F165as**]** in Article 2(12) of Commission Delegated Regulation (EU) 2015/962 supplementing Directive 2010/40/EU of the European Parliament and the Council with regard to the provision of EU-wide real-time traffic information services M65; and

(f) "Intelligent Transport Systems" has the same meaning as in Article 4(1) of Directive 2010/40/EU of the European Parliament and of the Council on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport M66.

The healthcare subsector

8.—(1) This paragraph describes the threshold requirements which apply to specified kinds of essential services in the healthcare settings sector.

(2) For the essential service of healthcare services the threshold requirements are—

(a) in England, an NHS Trust as defined in section 25 of the National Health Service Act 2006 M67 or a Foundation trust as defined in section 30 of the National Health Service Act 2006 M68;

(b) in Wales, a Local Health Board or NHS Trust as defined in the National Health Service (Wales) Act 2006 M69;

(c) in Scotland—

(i) the Common Services Agency for the Scottish Health Service established under section 10 of the National Health Service (Scotland) Act 1978 M70;

(ii) a Health Board, constituted under section 2 of the National Health Service (Scotland) Act 1978 M71; **[**F166and

(iii) a Special Health Board, constituted under section 2 of the National Health Service (Scotland) Act 1978;**]**

(d) in Northern Ireland, the Health and Social Care Trusts within the meaning of "HSC Trust" in section 31 of the Health and Social Care (Reform) Act (Northern Ireland) 2009 M72.

The drinking water supply and distribution subsector

9. The threshold requirement which applies to the essential service of the supply of potable water in the United Kingdom is the supply of water to 200,000 or more people.

The digital infrastructure subsector

10.—(1) This paragraph describes the threshold requirements which apply to specified kinds of essential services in the digital infrastructure subsector.

[F167(2) 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").

(3) 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.

(3A) 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.

(4) 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.**]**

(5) In this paragraph—

(a) "DNS" is a reference to "[F168Domain Name System]" which means a hierarchical distributed naming system [F168which processes and responds to queries for DNS resolution];

(b) "DNS service provider" is a reference to "[F169Domain Name System] service provider" which means an entity which provides DNS services [F169accessible via] the internet;

(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; F170...

[F171(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;]

(d) "TLD Name Registry" is a reference to "top-level domain name registry" which means an entity which administers and operates the registration of internet domain names under a specific top-level domain.

The data infrastructure subsector

11.—(1) This paragraph describes the threshold requirements which apply to specified kinds of essential services in the data infrastructure subsector.

(2) For the essential service of the provision of a data centre service in the United Kingdom, otherwise than on an enterprise basis, the threshold requirement is that the rated IT load of the data centre is equal to or greater than 1 megawatt.

(3) For the essential service of the provision of a data centre service in the United Kingdom on an enterprise basis, the threshold requirement is that the rated IT load of the data centre is equal to or greater than 10 megawatts.

(4) "Data centre service" means a service consisting of the provision of a physical structure (a "data centre") which—

(a) contains an area for the housing, connection and operation of relevant IT equipment, and

(b) provides supporting infrastructure for or in connection with the operation of relevant IT equipment.

(5) "Relevant IT equipment" means equipment used for the purposes of providing information technology services.

(6) "Supporting infrastructure" means one or more of the following—

(a) infrastructure for the supply of electricity;

(b) infrastructure for environmental control;

(c) infrastructure to ensure the security of the data centre and of relevant IT equipment in the data centre;

(d) infrastructure to ensure the resilience of the data centre and of relevant IT equipment in the data centre.

(7) A data centre service is provided on an enterprise basis if—

(a) the data centre is owned or managed by a person in connection with the carrying on of an undertaking by the person, and

(b) the sole purpose of the data centre is to provide information technology services for that undertaking.

(8) In this paragraph—

(a) "environmental control" includes heating, ventilation, air conditioning and control of matters such as airborne dust, humidity and flames;
(b) the "rated IT load" of a data centre is the maximum electrical power available for the operation of relevant IT equipment housed in the data centre;
(c) "structure" includes a building or part of a building, and references to a structure include references to a group of structures. *[(4) Data centres to be regulated as essential services]*

EXPLANATORY NOTE

(This note is not part of the Regulations)
These Regulations implement Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (OJ No L194, 19.7.2016, p1).
Part 2 of these Regulations provides a national framework for the security of network and information systems in the United Kingdom ("UK"). Under regulation 2, a Minister of the Crown must designate and publish a "national strategy" covering the sectors specified in column 1 of the table in Schedule 1 ("the relevant sectors") and digital services.
Regulation 3(1) designates national competent authorities, specified in column 3 of the table in Schedule 1, for the subsectors specified in column 2 of that table. Regulation 3(2) designates the Information Commissioner as the national competent authority for relevant digital service providers ("RDSPs"). The national competent authorities designated under regulation 3(1) and (2) (referred to as "NIS enforcement authorities") are required to carry out the duties mentioned in regulation 3(3), (4) and (6).
Regulation 4 designates the 'single point of contact' ("SPOC") for the UK and regulation 5 designates the UK's computer security incident response team for the relevant sectors and RDSPs.
Part 3 of these Regulations makes provision regarding the designation of operators of essential services and the duties which apply to them.
Under regulation 8, a person is identified as an operator of an essential service (an "OES") by virtue of either falling within regulation 8(1) or (3). A person is deemed to be an OES under regulation 8(1) if they provide an essential service of kind specified in paragraphs 1 to 9 of Schedule 2 which also satisfies the threshold requirements specified for that kind of essential service. A person may be designated by a competent authority as an OES if they meet the conditions mentioned in regulation 8(3)(a) to (c). The deemed designation of an OES under regulation 8(1), or designation of an OES under regulation 8(3), may be revoked by a competent authority under regulation 9. An OES must fulfil the security duties set out in regulation 10 and the duty to notify incidents set out in regulation 11.
Part 4 of these Regulations makes provision regarding the duties which apply to RDSPs and the Information Commissioner. This includes a duty on all RDSPs to register with the Information Commissioner.
Part 5 of these Regulations makes provision for powers of enforcement and penalties which apply to contraventions of the duties set out in these Regulations. Regulation 15 enables a competent authority to serve an information notice on an OES or any person to obtain information that it reasonably requires for specified purposes. Regulation 19 makes provision for the independent review of a decision to designate an OES or a decision to serve a penalty notice.
Part 6 of these Regulations makes provision about miscellaneous matters such as fees, proceeds of penalties, general considerations that apply to enforcement actions and service of documents.
Regulation 25 sets out a process for the Secretary of State to review the regulatory provision contained within these Regulations and publish a report setting out the conclusions of that review. The first such report must be published on or before 9th May 2020 and subsequent reviews must be carried out biennially after that date.
An impact assessment has been produced by the Department for Digital, Culture, Media and Sport and is published alongside the instrument at www.legislation.gov.uk.
An Explanatory Memorandum and a Transposition Note are published alongside the instrument at www.legislation.gov.uk.
The Directive referred to above is published at http://eur-lex.europa.eu.

Changes to legislation:
There are currently no known outstanding effects for the The Network and Information Systems Regulations 2018.