Cyber Security and Resilience (Network and Information Systems) Bill

[AS AMENDED ON REPORT]

CONTENTS

PART 1

INTRODUCTION

1 Meaning of "the NIS Regulations"
2 Overview of Act

PART 2

THE NIS REGULATIONS

CHAPTER 1

PERSONS REGULATED UNDER THE NIS REGULATIONS

Operators of essential services

3 Identification of operators of essential services
4 Data centres to be regulated as essential services
5 Operators of data centre services: Crown application etc
6 Designation of large load controllers as operators of an essential service

Providers of digital services

7 Digital services
8 Duties of relevant digital service providers

Providers of managed services

9 Managed service providers
10 Duties of managed service providers to manage risks

Persons subject to public authority oversight

11 Digital or managed service providers: meaning of "subject to public authority oversight"

Critical suppliers

12 Critical suppliers

CHAPTER 2

PROVISION OF INFORMATION AND REPORTING OF INCIDENTS

Information to be provided by regulated persons

13 Provision of information by operators of data centre services
14 Provision of information by providers of digital or managed services etc

Reporting of incidents by regulated persons

15 Reporting of incidents by regulated persons
16 Notification of incidents to customers

CHAPTER 3

OTHER AMENDMENTS

Cost recovery

17 Powers to impose charges

Information sharing

18 Sharing and use of information under the NIS Regulations etc

Guidance

19 Guidance

Investigatory powers, enforcement and penalties

20 Powers to require information
21 Financial penalties
22 Enforcement and appeals

Other

23 Minor and consequential amendments etc

PART 3

SECURITY AND RESILIENCE OF SYSTEMS: FUNCTIONS OF THE SECRETARY OF STATE

CHAPTER 1

INTRODUCTORY

24 Key definitions in Part 3

CHAPTER 2

STATEMENT OF STRATEGIC PRIORITIES ETC

25 Statement of strategic priorities etc
26 Consultation and procedure in relation to statement
27 Duties of regulatory authorities in relation to statement
28 Report by Secretary of State

CHAPTER 3

REGULATIONS ABOUT SECURITY AND RESILIENCE OF SYSTEMS

29 Regulations relating to security and resilience of network and information systems
30 Imposition of requirements on regulated persons
31 Functions of regulatory authorities: enforcement, sanctions and appeals
32 Functions of the Secretary of State: loss of control of artificial intelligence agent
33 Provision about financial penalties
34 Regulatory authorities, the Secretary of State and other persons: information, guidance and other functions
35 Recovery of costs of regulatory authorities
36 Supplementary provision and interpretation

CHAPTER 4

CODE OF PRACTICE

37 Code of practice
38 Procedure for issue of code of practice
39 Effects of code of practice
40 Withdrawal of code of practice

CHAPTER 5

REPORT ON NETWORK AND INFORMATION SYSTEMS LEGISLATION

41 Report on network and information systems legislation

CHAPTER 6

REGULATIONS UNDER PART 3

42 Regulations under section 24 or Chapter 3
43 Consultation and procedure

PART 4

DIRECTIONS FOR NATIONAL SECURITY PURPOSES

CHAPTER 1

VENDOR-RELATED DIRECTIONS ETC

44 Vendor-related directions
45 Further provision about giving of vendor-related directions
46 Power to make regulations about time frame for giving vendor-related directions
47 Power to establish mandatory referral scheme

CHAPTER 2

GENERAL DIRECTIONS

48 General directions

CHAPTER 3

DIRECTIONS UNDER SECTIONS 44 AND 48: SUPPLEMENTARY PROVISION

Compliance with directions to take priority

49 Compliance with directions under section 44 or 48 to take priority

Monitoring of compliance with directions

50 Monitoring by regulatory authorities

Information gathering and inspections

51 Information gathering
52 Inspections

Enforcement of requirements

53 Notification of contravention
54 Penalty amounts
55 Enforcement of notification
56 Enforcement of penalty
57 Enforcement of non-disclosure requirements

CHAPTER 4

DIRECTIONS TO REGULATORY AUTHORITIES

58 Power to direct regulatory authorities

CHAPTER 5

GENERAL PROVISION

59 Review, variation and revocation of directions
60 Publication of notice of direction under section 44 etc
61 Annual report in relation to directions under section 44
62 Laying before Parliament: directions under sections 48 and 58 etc
63 Information sharing
64 Means of giving directions, notices etc
65 Interpretation of Part 4
66 Review of the effectiveness of the NIS regime
67 Register of foreign powers for the purposes of Part 4

PART 5

GENERAL

68 Extent
69 Commencement
70 Short title

Schedule 1 — Enforcement and appeals
Schedule 2 — Minor and consequential amendments etc

[AS AMENDED ON REPORT]

A

B I L L

TO

Make provision, including provision amending the Network and Information Systems Regulations 2018, about the security and resilience of network and information systems used or relied on in connection with the carrying on of essential activities.

BE IT ENACTED by the King's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

PART 1

INTRODUCTION

1 Meaning of "the NIS Regulations"

In this Act, "the NIS Regulations" means the Network and Information Systems Regulations 2018 (S.I. 2018/506).

2 Overview of Act

(1) Part 2 of this Act contains amendments to the NIS Regulations.

(2) Those amendments include amendments—

(a) extending the application of the NIS Regulations to persons providing data centres, persons providing services relating to load control, and persons providing managed services;

(b) providing for the designation of persons as critical suppliers in relation to persons regulated by the NIS Regulations;

(c) relating to the reporting of incidents;

(d) relating to the recovery of costs, the sharing and gathering of information, and enforcement.

(3) Part 3 of this Act contains provision conferring powers on the Secretary of State—

(a) to specify activities to be regulated and to designate regulatory authorities to carry out that regulation (see Chapter 1 of that Part);

(b) to designate a statement of strategic priorities in relation to the security and resilience of network and information systems which are used or relied on in connection with the carrying on of essential activities (see Chapter 2 of that Part);

(c) to make regulations relating to the security and resilience of network and information systems which are used or relied on in connection with the carrying on of essential activities (see Chapter 3 of that Part);

(d) to issue a code of practice for persons with duties under regulations made under Chapter 3 of that Part or under the NIS Regulations (see Chapter 4 of that Part).

(4) Chapter 5 of Part 3 requires the Secretary of State to report on legislation relating to the security and resilience of network and information systems.

(5) Part 4 confers powers on the Secretary of State to give directions in particular circumstances involving a risk to national security interests.

PART 2

THE NIS REGULATIONS

CHAPTER 1

PERSONS REGULATED UNDER THE NIS REGULATIONS

Operators of essential services

3 Identification of operators of essential services

(1) Regulation 8 of the NIS Regulations (identification of operators of essential services) is amended as follows.

(2) After paragraph (1) insert—

"(1ZA) Paragraph (1) applies to a person whether or not the person is established in the United Kingdom."

(3) For paragraph (1A) substitute—

"(1A) Paragraph (1) does not apply to a person in relation to the provision by the person of 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)."

(4) After paragraph (3) insert—

"(3A) A person may be designated under paragraph (3) whether or not the person is established in the United Kingdom."

4 Data centres to be regulated as essential services

(1) The NIS Regulations are amended as follows.

(2) In the table in Schedule 1 (designated competent authorities), after the entry relating to digital infrastructure insert –

"Data infrastructure	Data infrastructure	The Office of Communications (United Kingdom)".

(3) In Schedule 2 (essential services and threshold requirements), after paragraph 10 insert –

"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."

5 Operators of data centre services: Crown application etc

In regulation 8 of the NIS Regulations (identification of operators of essential services), before paragraph (7A) insert—

"(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."

6 Designation of large load controllers as operators of an essential service

(1) Paragraph 1 of Schedule 2 to the NIS Regulations (essential services and threshold requirements: electricity subsector) is amended as follows.

(2) After sub-paragraph (5) insert—

"(5A) For the essential service of load control, the threshold requirement in the United Kingdom is a load controller—

(a) which carries on activities for system-balancing purposes (whether or not it also carries on other activities), and

(b) 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) an activity is carried on for "system-balancing purposes" if it is carried on with a view to contributing to the balancing, flexibility, security or stability of the electricity system as a whole or a significant part of it;

(b) "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;

(c) 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;

(d) 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."

(3) In sub-paragraph (8)—

(a) after paragraph (a) insert—

"(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) after paragraph (c) insert—

"(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;

(vi) a heat battery;";

(c) after paragraph (g) insert—

"(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;".

Providers of digital services

7 Digital services

(1) Regulation 1 of the NIS Regulations (interpretation etc) is amended as follows.

(2) Paragraph (2) is amended in accordance with subsections (3) to (6).

(3) For the definition of "cloud computing service" substitute—

""cloud computing service" means a digital service—

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

(i) there is 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;".

(4) Omit the definitions of "digital service" and "digital service provider".

(5) After the definition of "online search engine" insert—

""relevant digital service" means an online marketplace, an online search engine or a cloud computing service;".

(6) In the definition of "representative", for "a digital service provider" substitute "an RDSP".

(7) After paragraph (2) insert—

"(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 computing resources is "scalable" if the resources are flexibly allocated by the provider of the service, irrespective of the geographical location of the resources, in order to handle fluctuations in demand;

(c) a pool of computing resources is "elastic" if the resources are provided and released according to demand, in order to rapidly increase and decrease available resources depending on workload;

(d) computing resources are "shareable" if—

(i) multiple users share a common access to the service, which is provided from the same electronic equipment, and

(ii) processing is carried out separately for each user."

(8) In paragraph (3), for sub-paragraph (e) substitute—

"(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 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;".

(9) After paragraph (3) insert—

"(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)."

8 Duties of relevant digital service providers

(1) Regulation 12 of the NIS Regulations (relevant digital service providers) is amended as follows.

(2) In paragraph (2)—

(a) in sub-paragraph (b), for "their network and information systems with a view to ensuring the continuity of those services" substitute "the security of network and information systems referred to in paragraph (1)";

(b) omit sub-paragraph (c) (together with the "and" at the end of sub-paragraph (b)).

(3) After paragraph (2) insert—

"(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)."

Providers of managed services

9 Managed service providers

(1) The NIS Regulations are amended as follows.

(2) Regulation 1 (interpretation etc) is amended in accordance with subsections (3) to (5).

(3) In paragraph (2), after the definition of "incident" insert—

""managed service" has the meaning given by paragraph (3B);".

(4) In paragraph (3), after sub-paragraph (e) insert—

"(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;".

(5) After paragraph (3A) (inserted by section 7(9)) insert—

"(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

(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.

(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.

(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)."

(6) Regulation 3 (designation of competent authorities) is amended in accordance with subsections (7) and (8).

(7) In paragraph (2), after "RDSPs" insert "and for RMSPs".

(8) In paragraph (4)—

(a) after "In relation to" insert "relevant";

(b) after "services" insert "and managed services".

10 Duties of managed service providers to manage risks

After regulation 14A of the NIS Regulations insert—

"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)."

Persons subject to public authority oversight

11 Digital or managed service providers: meaning of "subject to public authority oversight"

In regulation 1 of the NIS Regulations, after paragraph (3D) (inserted by section 9(5)) insert—

"(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."

Critical suppliers

12 Critical suppliers

(1) The NIS Regulations are amended as follows.

(2) In regulation 1(2) (interpretation etc), after the definition of "Cooperation Group" insert—

""critical supplier" means a person for the time being designated under regulation 14H;".

(3) After regulation 14G (inserted by section 16(4) below) insert—

"PART 4B

Critical suppliers

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.

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)—

(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.

Revocation of designation

14K. – (1) Where a designated competent authority has designated a person 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

(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.

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."

CHAPTER 2

PROVISION OF INFORMATION AND REPORTING OF INCIDENTS

Information to be provided by regulated persons

13 Provision of information by operators of data centre services

(1) The NIS Regulations are amended as follows.

(2) After regulation 8 insert—

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

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

(a) 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) 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."

(3) In regulation 8A (nomination by an OES of a person to act on its behalf in the United Kingdom), in paragraph (1)(a)—

(a) for "and 10" substitute ", 10 and 11", and

(b) for "or digital" substitute ", digital or data".

14 Provision of information by providers of digital or managed services etc

(1) The NIS Regulations are amended as follows.

(2) In regulation 14 (registration with the Information Commission)—

(a) in paragraph (2), for sub-paragraph (b) substitute—

"(b) the RDSP's proper address;

(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;

(bc) which relevant digital services the RDSP provides;";

(b) after paragraph (2) insert—

"(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.";

(c) in paragraph (3), for the words from "as soon as possible" to the end substitute "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.";

(d) for paragraph (4) substitute—

"(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.";

(e) after that paragraph insert—

"(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."

(3) Regulation 14A (representatives of digital service providers established outside the United Kingdom) is amended in accordance with subsections (4) to (8).

(4) For paragraph (1) substitute—

"(1) This regulation applies to an RDSP which has its principal office outside the United Kingdom."

(5) In paragraph (2)—

(a) for "digital service provider" substitute "RDSP";
(b) in sub-paragraph (b), after "representative" insert "(including an email address and telephone number)".

(6) For paragraphs (3) and (4) substitute—

"(3) The RDSP 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;

(b) in any other case, 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.

(4) 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 RDSP."

(7) In paragraph (5)—
(a) for "paragraph (1)" substitute "paragraph (2)";
(b) for "digital service provider" substitute "RDSP".

(8) In the heading, for "digital service providers" substitute "RDSPs".

(9) After regulation 14B (inserted by section 10) insert—

"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

(b) subsequently, at annual intervals.

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 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."

Reporting of incidents by regulated persons

15 Reporting of incidents by regulated persons

(1) The NIS Regulations are amended as follows.

(2) In regulation 1(2) (interpretation), in the definition of "incident", after "on the" insert "operation or".

(3) For regulation 11 substitute—

"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 the essential 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.

(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.

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 (5) in relation to the incident, so far as known to the OES.

(3) In this regulation, "data centre incident" means an incident which 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, or

(b) a significant impact, by virtue of its effect on network and information systems falling within paragraph (4), on the operation or security of the data centre service provided by the OES in the United Kingdom.

(4) A network and information system falls within this paragraph if –

(a) it is relied on by the OES to provide the data centre service, or

(b) it is a network and information system of a customer of the data centre service.

(5) 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 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 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.

(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.

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) 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."

(4) In regulation 12 (relevant digital service providers)—

(a) omit paragraphs (3) to (9) and (11) to (16);

(b) in the heading, after "providers" insert ": duties to manage risks to network and information systems".

(5) After regulation 12 insert—

"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—

(a) 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;

(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 the relevant digital 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 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.

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

(b) the SPOC, or

(c) the CSIRT."

(6) In regulation 13 (co-operation with European Union), for "12(3)" substitute "12A".

(7) After regulation 14D (inserted by section 14) insert—

"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 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;

(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.

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."

16 Notification of incidents to customers

(1) The NIS Regulations are amended as follows.

(2) After regulation 11B (inserted by section 15(3)) insert—

"Incidents: notification 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

(b) explain why the OES considers that the customer is likely to be adversely affected by the incident.

(5) After the OES has notified customers under paragraph (2)(b), the OES must provide them with such updates about the incident and its impact as the OES considers necessary."

(3) After regulation 12B (inserted by section 15(5)) insert—

"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.

(4) After the RDSP has notified customers under paragraph (1)(b), the RDSP must provide them with such updates about the incident and its impact as the RDSP considers necessary."

(4) After regulation 14F (inserted by section 15(7)) insert—

"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

(b) explain why the RMSP considers that the customer is likely to be adversely affected by the incident.

(4) After the RMSP has notified customers under paragraph (1)(b), the RMSP must provide them with such updates about the incident and its impact as the RMSP considers necessary."

CHAPTER 3

OTHER AMENDMENTS

Cost recovery

17 Powers to impose charges

After regulation 20 of the NIS Regulations insert—

"PART 5A

Powers to impose charges

Periodic charges under charging schemes

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 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 has effect.

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).

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)."

Information sharing

18 Sharing and use of information under the NIS Regulations etc

(1) In regulation 3 of the NIS Regulations (designation of national competent authorities)—

(a) in paragraph (3)(e), for the words from ", as the SPOC" to the end substitute "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;";

(b) after paragraph (5) insert—

"(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 day on which section 18(1) of the Cyber Security and Resilience

(Network and Information Systems) Act 2026 comes into force, and

(b) subsequently, at annual intervals."

(2) In regulation 4 of the NIS Regulations (single point of contact)—

(a) in paragraph (2), for "Member State of the EU" substitute "country or territory outside the United Kingdom";

(b) after paragraph (2) insert—

"(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."

(3) For regulation 6 of the NIS Regulations substitute—

"Sharing of information

6.—(1) A NIS enforcement authority may disclose to another NIS enforcement authority or to a person within paragraph (2) information obtained in the exercise of its functions—

(a) for the purposes of these Regulations or of facilitating the exercise by 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),

(b) otherwise in connection with—

(i) the security or resilience of network and information systems, or

(ii) any other matter relating to cyber security or resilience,

(c) for national security purposes,

(d) in connection with the prevention or detection of crime (whether or not in the United Kingdom),

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

(f) 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 sub-paragraphs (a) to (c).

(3) But a NIS enforcement authority may disclose information under paragraph (1) to a relevant law-enforcement authority which is established in a country or territory outside the United Kingdom only if the country or territory in which the relevant law-enforcement authority is established is listed in paragraph (4).

(4) The countries and territories are—

Australia;

Canada;

an EEA state;

New Zealand;

Switzerland;

the United States of America.

(5) 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.

(6) 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 41 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 the provision and availability of data centre services in the United Kingdom, or

(c) may assist the Secretary of State in formulating policy relating to—

(i) the provision and availability of data centre services in the United Kingdom, or

(ii) national security.

(7) 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 41 of the Cyber Security and Resilience (Network and Information Systems) Act 2026,

(b) in assessing the provision and availability of data centre services in the United Kingdom, or

(c) in formulating policy relating to anything mentioned in paragraph (6)(c).

(8) A NIS enforcement authority may disclose information obtained by the authority in the exercise of its functions to a relevant overseas authority if the disclosure is for a purpose mentioned in paragraph (1).

(9) In paragraph (8), a "relevant overseas authority", in relation to a disclosure by a NIS enforcement authority, means a person established in a country or territory listed in paragraph (4) 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

(b) relate to any of the matters mentioned in paragraph (1)(b) to (f).

(10) 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.

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 (6).

(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), or

(ii) the person making the disclosure considers that any of sub-paragraphs (a) to (c) of regulation 6(6) 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).

(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) But relevant information may be disclosed under paragraph (2)(b) by a NIS enforcement authority to a relevant law-enforcement authority which is established in a country or territory outside the United Kingdom only if the

country or territory in which the relevant law-enforcement authority is established is listed in paragraph (5).

(5) The countries and territories are—

Australia;

Canada;

an EEA state;

New Zealand;

Switzerland;

the United States of America.

(6) 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.

(7) But relevant information may be disclosed under paragraph (6) by a NIS enforcement authority to a person established in a country or territory outside the United Kingdom only if the country or territory in which the person is established is listed in paragraph (5).

(8) A disclosure of information under any provision of regulation 6 or this regulation must be limited to information which is relevant and proportionate to the purpose for which the disclosure is being made.

(9) 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).

(10) 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.

(11) Regulation 6 and this regulation do not limit the circumstances in which information may be disclosed apart from those regulations.

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."

(4) In regulation 7 of the NIS Regulations (information sharing - Northern Ireland), after paragraph (1) insert—

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

(1B) 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).

(1C) 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."

Guidance

19 Guidance

(1) The NIS Regulations are amended as follows.

(2) Regulation 3 (designation of national competent authorities) is amended in accordance with subsections (3) to (5).

(3) After paragraph (3) insert—

"(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

(b) consult each of the other designated competent authorities and the Information Commission before publishing the guidance."

(4) After paragraph (4) insert—

"(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."

(5) After paragraph (6) insert—

"(7) In this regulation, "relevant code" means a code of practice issued under section 37 of the Cyber Security and Resilience (Network and Information Systems) Act 2026."

(6) After regulation 3 insert—

"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."

Investigatory powers, enforcement and penalties

20 Powers to require information

(1) The NIS Regulations are amended as follows.

(2) In the heading of Part 5, for "Enforcement" substitute "Information, enforcement".

(3) For regulation 15 substitute—

"Information gathering

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) assessing the security or resilience of network and information systems relied on by a person regulated by the designated competent authority;

(f) establishing whether any incident has occurred that the designated competent authority believes could have had, has had, is having or is likely to have, an adverse effect on the security or resilience of network and information systems relied on by a person regulated by the authority, and the nature and impact of any such incident;

(g) assessing the implementation of measures taken under regulation 10 to manage risks and to prevent and minimise the impact of incidents, including as a result of any inspection conducted under regulation 16;

(h) identifying a failure of a person to comply with any duty imposed by these Regulations;

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

(j) 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) assessing the security or resilience of network and information systems relied on by a person regulated by the Information Commission;

(f) establishing whether any incident has occurred that the Information Commission believes could have had, has had, is having or is likely to have, an adverse effect on the security or resilience of network and information systems relied on by a person regulated by the Commission, and the nature and impact of any such incident;

(g) assessing the implementation of measures taken under regulation 12 or 14B to manage risks and to prevent and minimise the impact of incidents, including as a result of any inspection conducted under regulation 16;

(h) identifying a failure of a person to comply with any duty imposed by these Regulations;

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

(j) 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).

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, or

(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."

21 Financial penalties

(1) Regulation 18 of the NIS Regulations (penalties) is amended as follows.

(2) After paragraph (2) insert—

"(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

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

(3) For paragraphs (3A) and (3B) substitute—

"(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."

(4) In paragraph (3C)—

(a) after "penalty notice" insert "on a person";

(b) for "the OES or RDSP" substitute "the person";

(c) for "regulation 17(1) or (2)" substitute "regulation 17".

(5) In paragraph (3D)(a) and (c), for "OES or RDSP" (in each place it occurs) substitute "person to which it relates".

(6) In paragraph (3E)—

(a) for "OES or RDSP" substitute "person served with a penalty notice";

(b) for "a penalty notice" substitute "the notice".

(7) For paragraphs (5) to (7) substitute—

"(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(8));

(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);

(vii) sub-paragraph (ch) (failure to comply with regulation 11C(5));

(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 12C(4));

(iv) sub-paragraph (dzd) (failure to comply with regulation 14(2) or (3));

(v) 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);

(v) sub-paragraph (j) (failure to comply with regulation 14G(4)).

(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(6) and (7) 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));

(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 (k) (failure to comply with a direction under regulation 16(2)(c));

(vii) sub-paragraph (l) (failure to comply with regulation 16(3));

(d) regulation 17(2ZB) (failure to comply with information notice);

(e) regulation 17(3A) (failure to comply with requirements of enforcement notice)."

22 Enforcement and appeals

Schedule 1 contains further amendments to the NIS Regulations in connection with enforcement and appeals.

Other

23 Minor and consequential amendments etc

Schedule 2 contains minor and consequential amendments to the NIS Regulations and other enactments.

PART 3

SECURITY AND RESILIENCE OF SYSTEMS: FUNCTIONS OF THE SECRETARY OF STATE

CHAPTER 1

INTRODUCTORY

24 Key definitions in Part 3

(1) In this Part, "network and information system" means—

(a) an electronic communications network within the meaning of section 32(1) of the Communications Act 2003, or

(b) apparatus which is programmed to process digital data.

(2) A reference in subsection (1) to an electronic communications network or to apparatus includes a reference to data stored, processed, retrieved or transmitted by the network or apparatus for the purposes of the operation, use, protection or maintenance of the network or apparatus.

(3) In this Part, "essential activity" means an activity specified for the purposes of this subsection in regulations made by the Secretary of State.

(4) An activity may be specified for the purposes of subsection (3) only if the Secretary of State considers that the carrying on of the activity is essential to—

(a) the economy of the United Kingdom or any part of the United Kingdom, or

(b) the day-to-day functioning of society in the United Kingdom or any part of the United Kingdom.

(5) For the purposes of this Part—

(a) references to the carrying on of an activity include references to the provision of a service (and references to an activity include references to a service);

(b) the following are to be treated for the purposes of this Part as activities specified for the purposes of subsection (3)—

(i) an essential service (within the meaning of the NIS Regulations) specified in Schedule 2 to those Regulations;

(ii) a service which is deemed by regulation 8(2A) of those Regulations to be an essential service;

(iii) a relevant digital service (within the meaning of those Regulations);

(iv) a managed service (within the meaning of those Regulations).

(6) In this Part, "regulatory authority" means a person designated for the purposes of this subsection by regulations made by the Secretary of State.

(7) A person may be designated for the purposes of subsection (6) only if the person exercises functions of a public nature in the United Kingdom.

(8) The following persons are to be treated for the purposes of this Part as having been designated for the purposes of subsection (6)—

(a) a person designated by regulation 3(1) of the NIS Regulations (competent authorities for operators of essential services);

(b) the Information Commission.

(9) For the meaning of "regulated person" (in Chapters 3 and 4) see section 30(2).

CHAPTER 2

STATEMENT OF STRATEGIC PRIORITIES ETC

25 Statement of strategic priorities etc

(1) The Secretary of State may designate a statement for the purposes of this section if the requirements set out in section 26 (consultation and procedural requirements) are satisfied.

(2) The statement is a statement prepared by the Secretary of State that sets out—

(a) the strategic priorities of His Majesty's Government in relation to the security and resilience of network and information systems used or relied on in connection with the carrying on of essential activities,

(b) the roles and responsibilities of regulatory authorities and other persons involved in giving effect to these priorities, and

(c) objectives for regulatory authorities in seeking to give effect to those priorities.

(3) The Secretary of State must publish a statement designated under subsection (1) in such manner as the Secretary of State considers appropriate.

(4) A statement designated under subsection (1) may be amended (including by replacing the whole or a part of the statement with new material, or by withdrawing part of the statement) by a subsequent statement designated under that subsection, and this section and section 26 apply in relation to any subsequent statement as they apply in relation to the original statement.

(5) The designation of a statement under subsection (1) may be withdrawn by the Secretary of State.

(6) Except as provided by subsection (7), no amendment of a statement under subsection (4) or withdrawal of a designation under subsection (5) may be made within the period of three years beginning with the day on which a statement was most recently designated under subsection (1).

(7) An earlier amendment of a statement under subsection (4) or withdrawal of a designation under subsection (5) may be made if since that day—

(a) a Parliamentary general election has taken place, or

(b) the Secretary of State considers that there has been a significant change in—

(i) the policy of His Majesty's Government relating to the security and resilience of network and information systems used or relied on in connection with the carrying on of essential activities, or

(ii) the nature of threats to the security and resilience of such network and information systems.

(8) For the purposes of this section, corrections of clerical or typographical errors are not to be treated as amendments made to the statement.

26 Consultation and procedure in relation to statement

(1) This section sets out the requirements that must be satisfied in relation to a statement before the Secretary of State may designate it under section 25(1).

(2) The Secretary of State must consult the regulatory authorities on a draft of the statement.

(3) The Secretary of State must allow the regulatory authorities a period of at least 40 days to respond to the consultation.

(4) After that period has ended the Secretary of State—

(a) must make any changes to the draft that appear to the Secretary of State to be appropriate in light of responses to the consultation, and

(b) must then lay the statement before Parliament.

(5) The Secretary of State must wait until the end of the 40-day period and may not designate the statement if, within that period, either House of Parliament resolves not to approve it.

(6) "The 40-day period" is the period of 40 days beginning with the day on which the statement is laid before Parliament (or, if it is not laid before each House on the same day, the later of the days on which it is laid).

(7) In calculating the 40-day period, no account is to be taken of any period during which Parliament is dissolved or prorogued or during which both Houses are adjourned for more than 4 days.

(8) Subsections (2) and (3) may be satisfied by consultation carried out before the coming into force of this section.

27 Duties of regulatory authorities in relation to statement

(1) This section applies where a statement is for the time being designated under section 25(1).

(2) Each regulatory authority must, when exercising any of its functions under or by virtue of the legislation mentioned in subsection (3)—

(a) have regard to the statement, and

(b) seek to achieve any relevant objectives set out in the statement.

(3) The legislation referred to in subsection (2) is—

(a) the NIS Regulations, and

(b) this Part and Part 4.

28 Report by Secretary of State

(1) The Secretary of State must, after the end of each reporting period, lay before Parliament a report setting out, in general terms, how regulatory authorities—

(a) have complied with their duties under section 27 during the reporting period, and

(b) are planning to comply with their duties under that section during the subsequent reporting period.

(2) The Secretary of State must publish a report under subsection (1) in such manner as the Secretary of State considers appropriate.

(3) In this section, "reporting period" means—

(a) the period of 12 months beginning with the day on which the first statement designated under section 25(1) is published under section 25(3), and

(b) each subsequent period of 12 months.

(4) The Secretary of State may by notice require a regulatory authority to provide the Secretary of State with such information for the purposes of a report under subsection (1) as may be specified in the notice.

(5) A regulatory authority to which a notice is given under subsection (4) must provide the information by such time and in such form as may be specified in the notice.

CHAPTER 3

REGULATIONS ABOUT SECURITY AND RESILIENCE OF SYSTEMS

29 Regulations relating to security and resilience of network and information systems

(1) The Secretary of State may by regulations make provision for the purposes of or in connection with the following objectives—

(a) the identification, management and reduction of risks of security or operational compromises in relation to relevant network and information systems;

(b) the mitigation of adverse impacts resulting from such security or operational compromises.

(2) Provision for the purposes of or in connection with the objectives mentioned in subsection (1) may in particular include provision with a view to strengthening the resilience of relevant network and information systems and the resilience and security of their surrounding physical environment.

(3) For the purposes of this Chapter, a network and information system is "relevant" if—

(a) it is used or relied on in connection with the carrying on of an essential activity or the provision of an activity-critical supply, or

(b) it is associated with a system to which paragraph (a) applies.

(4) A network and information system is "associated" with a system to which subsection (3)(a) applies if the occurrence of a security or operational compromise in relation to either of those systems would be likely to put the other system at increased risk of a security or operational compromise.

(5) In this Chapter, "security or operational compromise", in relation to a network and information system, means—

(a) anything that compromises the security, availability, functionality or reliability of the system,

(b) any unauthorised access to, interference with or exploitation of the system or anything which enables such access, interference or exploitation,

(c) anything that compromises the confidentiality, authenticity, integrity or availability of data stored on or processed, received or transmitted by the system, or

(d) anything that causes data stored on or processed by the system to be lost.

(6) In this Chapter, "activity-critical supply" means a supply of goods or services without which the carrying on of an essential activity would be at risk of disruption.

30 Imposition of requirements on regulated persons

(1) Regulations under section 29(1) may impose requirements on regulated persons.

(2) In this Chapter, "regulated person" means a person specified, or of a description specified, for the purposes of this subsection.

(3) A person or description may be specified for the purposes of subsection (2) only if the person, or every person of that description—

(a) carries on an essential activity in the United Kingdom, or

(b) provides an activity-critical supply,

(whether or not the person is established in the United Kingdom).

(4) Provision made by virtue of subsection (2) may in particular be framed by reference to whether the person, or every person of that description, is for the time being designated by a regulatory authority in accordance with provision made by regulations under section 29(1).

(5) The following are to be treated as having been specified for the purposes of subsection (2)—

(a) an operator of an essential service (within the meaning of the NIS Regulations);

(b) a relevant digital service provider (within the meaning of those Regulations);

(c) a relevant managed service provider (within the meaning of those Regulations);

(d) a critical supplier (within the meaning of those Regulations).

(6) The requirements which may be imposed by virtue of subsection (1) include, in particular—

(a) requirements to take specified action, or action of a specified description, for the purposes of or in connection with an objective mentioned in section 29(1) (and such measures may include measures outside the United Kingdom);

(b) requirements in the form of prohibitions or restrictions relating to the taking of specified action or action of a specified description;

(c) requirements relating to the reporting of specified matters;

(d) requirements to provide information to regulatory authorities, the Secretary of State and other persons;

(e) requirements relating to the appointment of a representative in the United Kingdom (in the case of a regulated person established outside the United Kingdom).

(7) In this section, "specified" means specified in regulations under section 29(1).

31 Functions of regulatory authorities: enforcement, sanctions and appeals

(1) Regulations under section 29(1) may confer functions on regulatory authorities in connection with—

(a) monitoring compliance with relevant requirements;

(b) investigating suspected non-compliance with relevant requirements;

(c) securing compliance with relevant requirements;

(d) mitigating the effect of non-compliance with relevant requirements.

(2) "Relevant requirement" means a requirement imposed under or by virtue of—

(a) regulations under section 29(1), or

(b) the NIS Regulations.

(3) Provision made by virtue of subsection (1) may include provision—

(a) conferring power on a regulatory authority to appoint inspectors to carry out functions under the regulations;

(b) conferring functions on a regulatory authority or an inspector, including power—

(i) to enter, inspect and search premises;

(ii) to seize and retain documents, information or other things which may be relevant to the carrying out of functions under the regulations;

(iii) to require a person to obtain, generate, collect or retain documents or information (including documents or information outside the United Kingdom) or other things which may be relevant to the carrying out of functions under the regulations;

(iv) to carry out tests or interviews;

(v) to require a person to take steps (including steps outside the United Kingdom) for the purpose of demonstrating compliance with a relevant requirement or remedying or mitigating a failure to comply with such a requirement.

(4) Regulations under section 29(1) which confer any power described in subsection (3)(b) may impose conditions relating to the exercise of the power, including for example conditions requiring a person exercising the power—

(a) to produce evidence of their identity or authority;

(b) to obtain a warrant from a person specified in the regulations before exercising the power.

(5) Provision made by virtue of subsection (1) may include provision conferring powers on regulatory authorities for or in connection with sanctions, including financial penalties, for non-compliance with relevant requirements.

(6) Regulations under section 29(1)—

(a) must, where they provide for financial penalties, make provision about appeals to a court or tribunal against the imposition of such a penalty;

(b) may make provision about appeals to a court or tribunal against decisions or actions (including the imposition of a sanction other than a financial penalty) under or by virtue of the regulations.

(7) The provision that may be made in reliance on subsection (6) includes provision—

(a) about the grounds on which an appeal may be made;

(b) about the procedure for making an appeal (including any fee that may be payable);

(c) suspending the effect of any decision, penalty or other action pending determination of the appeal;

(d) about the powers of the court or tribunal to which an appeal is made;

(e) for the recovery (whether by action on a debt or otherwise) of any sum payable in pursuance of a decision of the court or tribunal.

(8) Provision referred to in subsection (7)(d) includes provision conferring on the court or tribunal to which an appeal is made power—

(a) to confirm a financial penalty;

(b) to withdraw a financial penalty;

(c) to vary the amount of a financial penalty;

(d) to award costs.

32 Functions of the Secretary of State: loss of control of artificial intelligence agent

(1) Regulations under section 29(1) may confer functions on the Secretary of State in connection with cases where—

(a) a security or operational compromise in relation to a relevant network and information system is or may be attributable to loss of oversight or control of an AI agent, or

(b) there is a risk of a security or operational compromise of a kind described in paragraph (a).

(2) In this section—

(a) "AI agent" has the meaning given by regulations made by the Secretary of State;

(b) references to loss of oversight or control, in relation to an AI agent, have the meaning given by regulations made by the Secretary of State;

(c) references to an AI-related compromise are to a security or operational compromise of a kind described in subsection (1)(a).

(3) Provision referred to in subsection (2)(a) may, in particular, be framed by reference to—

(a) whether a thing has, or does not have, functionalities or other features specified in the regulations;

(b) whether a thing has, or does not have, characteristics or capabilities specified in the regulations.

(4) Provision referred to in subsection (2)(b) may, in particular, be framed by reference to circumstances in which a security or operational compromise is to be taken to be, or not to be, attributable to loss of oversight or control of an AI agent.

(5) The functions that may be conferred by virtue of subsection (1) include, in particular, functions in relation to the imposition of requirements on regulated persons or the taking of other action in connection with—

(a) identifying and investigating AI-related compromises or risks of AI-related compromises;

(b) obtaining, preserving and analysing information;

(c) assessing the causes and effects of, and risks arising from, AI-related compromises;

(d) identifying, testing and verifying remedies and mitigations, and sharing assessments and information about remedies and mitigations, with a view to—

(i) preventing similar compromises or losses of oversight or control occurring in the future, or

(ii) mitigating the impact of AI-related compromises;

(e) securing compliance with a requirement imposed on a regulated person in connection with the exercise of a function described in any of paragraphs (a) to (d);

(f) mitigating the effect of non-compliance by a regulated person with any such requirement.

(6) Provision made by virtue of subsection (5) may include provision—

(a) conferring power on the Secretary of State to appoint inspectors to carry out functions conferred by virtue of subsection (1);

(b) conferring functions on the Secretary of State or an inspector, including power—

(i) to enter, inspect and search premises of a regulated person;

(ii) to seize and retain documents, information or other things in relation to a regulated person;

(iii) to require a regulated person to obtain, generate, collect or retain documents or information (including documents or information outside the United Kingdom) or other things;

(iv) to carry out tests or interviews;

(v) to require a regulated person to take steps (including steps outside the United Kingdom) for a purpose within subsection (7).

(7) The purposes within this subsection are—

(a) enabling or assisting with the exercise of any function conferred by virtue of subsection (1);

(b) demonstrating compliance with a requirement imposed on a regulated person in connection with the exercise of any function conferred by virtue of subsection (1);

(c) remedying or mitigating a failure to comply with such a requirement.

(8) Regulations under section 29(1) which confer any power described in subsection (6)(b) may impose conditions relating to the exercise of the power, including for example conditions requiring a person exercising the power—

(a) to produce evidence of their identity or authority;

(b) to obtain a warrant from a person specified in the regulations before exercising the power.

(9) Provision made by virtue of subsection (1) may include provision conferring powers on the Secretary of State for or in connection with sanctions, including financial penalties, for non-compliance by regulated persons with requirements imposed in connection with the exercise of other functions conferred by virtue of subsection (1).

33 Provision about financial penalties

(1) Where regulations under section 29(1) make provision for or in connection with the imposition of financial penalties by regulatory authorities or the Secretary of State, the regulations—

(a) may specify the amount of a penalty or provide for how the amount of a penalty is to be determined;

(b) must, in providing for the imposition of a penalty, provide for how the person by whom the penalty is imposed deals with sums received by it towards payment of the penalty;

(c) may provide for the person by whom the penalty is imposed to recover (whether by action on a debt or otherwise) any unpaid part of a penalty payable to it.

(2) Regulations made by virtue of subsection (1)(a) may provide for the amount of a penalty payable by a person to be determined by reference to a daily rate.

(3) Regulations made by virtue of subsection (1)(a) must include provision about the maximum amount of a penalty payable by a person, which—

(a) where the person is an undertaking (within the meaning given by the regulations), may not exceed the greater of—

(i) £17,000,000, and

(ii) 10% of the turnover of the undertaking (both inside and outside the United Kingdom);

(b) in any other case, may not exceed £17,000,000,

and the regulations must include provision about how an undertaking's turnover is to be determined.

(4) Regulations that include provision within subsection (3) may, in particular—

(a) include provision that a person of a description specified in the regulations is or is not an undertaking;

(b) make provision about amounts which are, or are not, to be taken into account in determining an undertaking's turnover;

(c) make provision about the period by reference to which an undertaking's turnover is to be determined;

(d) make provision conferring a power on the Secretary of State to make a determination in a particular case in relation to matters mentioned in the regulations (including the matters mentioned in paragraphs (b) and (c));

(e) provide, in a case where an undertaking is a member of a group, for other members of the group to be treated as part of the undertaking for the purposes of determining the undertaking's turnover;

(f) provide, in a case where an undertaking controls or is controlled by another person, for that person to be treated as part of the undertaking for the purposes of determining the undertaking's turnover,

and references in paragraph (f) to control are to be construed in accordance with the regulations.

(5) The Secretary of State may by regulations amend an amount specified in subsection (3)(a)(i) or (b) for the purpose of reflecting inflation.

34 Regulatory authorities, the Secretary of State and other persons: information, guidance and other functions

(1) Regulations under section 29(1) may confer functions on regulatory authorities in connection with any of the following—

(a) the disclosure of information—

(i) between regulatory authorities;

(ii) by regulatory authorities to other persons (including persons outside the United Kingdom);

(iii) to regulatory authorities by other persons (including persons outside the United Kingdom);

(b) the giving of guidance;

(c) the keeping of records and registers;

(d) the preparation of reports;

(e) the carrying out of reviews;
(f) consultation and cooperation with other persons (including persons outside the United Kingdom).

(2) Where regulations under section 29(1) make provision by virtue of section 32(1), the regulations may confer functions on the Secretary of State in connection with any of the following—
(a) the disclosure of information—
(i) between the Secretary of State and regulatory authorities;
(ii) by the Secretary of State to other persons (including persons outside the United Kingdom);
(iii) to the Secretary of State by other persons (including persons outside the United Kingdom);
(b) the giving of guidance;
(c) the keeping of records and registers;
(d) the preparation of reports;
(e) the carrying out of reviews;
(f) consultation and cooperation with other persons (including persons outside the United Kingdom).

(3) Provision described in subsection (1)(a) or (2)(a) may include provision about—
(a) the circumstances in which, purposes for which and persons to which information may or must be disclosed;
(b) where the regulations authorise a person to require another person to disclose information, how such a requirement is to be imposed;
(c) the type of information which may or must be disclosed;
(d) restrictions on disclosure;
(e) how information disclosed may or may not be used.

(4) Except as provided by subsection (5), regulations under section 29(1) may provide for the processing of information in accordance with the regulations not to be in breach of—
(a) any obligation of confidence owed by the person processing the information, or
(b) any other restriction on the processing of the information (however imposed).

(5) Regulations under section 29(1) may not require or authorise the making of a disclosure which is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.

(6) Regulations under section 29(1) may confer functions on persons (other than regulatory authorities) which exercise functions of a public nature.

(7) Functions conferred by virtue of subsection (6) may include, in particular, functions in connection with—
(a) co-operating with, or consulting, other persons (including persons outside the United Kingdom);

(b) submitting reports and carrying out analyses;
(c) monitoring incidents relating to relevant network and information systems;
(d) publicising and providing information relating to relevant network and information systems;
(e) promoting best practice in relation to risk management and other matters relating to the security of relevant network and information systems.

35 Recovery of costs of regulatory authorities

(1) Regulations under section 29(1) may make provision for a regulatory authority to impose charges on persons which are or have been regulated persons in respect of their relevant costs.

(2) The "relevant costs" of a regulatory authority are its costs or expected costs in connection with the exercise of functions conferred under or by virtue of—
(a) this Part or Part 4, or
(b) the NIS Regulations,
including costs in connection with the enforcement of relevant requirements.

(3) Regulations made by virtue of subsection (1) may provide for the imposition of charges by a regulatory authority in accordance with a scheme made by the authority (a "charging scheme").

(4) Regulations made by virtue of subsection (1) may include provision, or authorise a charging scheme to include provision, about—
(a) the circumstances in which a charge is payable;
(b) the amount of a charge (including how an amount is to be calculated);
(c) matters which must or may be taken into account by a regulatory authority in calculating the amount of a charge;
(d) reductions, exemptions and waivers;
(e) how and when a charge is to be paid;
(f) the collection and recovery of payments;
(g) interest payable on outstanding payments;
(h) the resolution of disputes (including appeals to a court or tribunal).

(5) Regulations made by virtue of subsection (1) may provide, or authorise a charging scheme to provide, that a charge imposed on a person, or the amount of such a charge, need not relate to the exercise of functions in relation to the person.

(6) Provision made by virtue of subsection (4)(c) may in particular include provision about deficits previously incurred by a regulatory authority.

(7) Regulations made by virtue of subsection (1) may authorise a charging scheme to make different provision for different purposes (including different provision in relation to different persons or circumstances).

(8) In this section, "relevant requirement" has the same meaning as in section 31.

36 Supplementary provision and interpretation

(1) Regulations under section 29(1) may—

(a) confer functions involving the exercise of a discretion;

(b) provide for the delegation of functions by a regulatory authority or the Secretary of State;

(c) require a person to have regard to guidance or to a code of practice;

(d) make provision by reference to a document as amended from time to time.

(2) In this Chapter—

"activity-critical supply" has the meaning given by section 29(6);

"regulated person" has the meaning given by section 30(2);

"relevant network and information system" has the meaning given by section 29(3);

"security or operational compromise" has the meaning given by section 29(5).

(3) See also Chapter 6 (which contains further provision about regulations under this Part).

CHAPTER 4

CODE OF PRACTICE

37 Code of practice

(1) The Secretary of State may issue a code of practice for regulated persons describing measures recommended for the purposes of compliance with requirements imposed on them under or by virtue of—

(a) regulations under section 29(1), or

(b) the NIS Regulations.

(2) The Secretary of State may from time to time revise and reissue a code under this section.

(3) Before preparing or revising a code under this section, the Secretary of State must consult such persons as the Secretary of State considers appropriate.

(4) A code under this section—

(a) may make different provision for different purposes (including different provision for different descriptions of regulated persons);

(b) may contain transitional provisions and savings.

(5) In this Chapter, "regulated person" has the same meaning as in Chapter 3.

38 Procedure for issue of code of practice

(1) Before issuing or reissuing a code of practice under section 37, the Secretary of State must lay before Parliament a draft of the code as proposed to be issued or reissued.

(2) If, within the 40-day period, either House of Parliament resolves not to approve the draft laid under subsection (1)—
  (a) the Secretary of State must not issue or reissue the code in the form of that draft, and
  (b) the Secretary of State may prepare another code.

(3) If no such resolution is passed within the 40-day period, the Secretary of State may issue or reissue the code of practice.

(4) If the code is issued or reissued—
  (a) the Secretary of State must publish it, and
  (b) the code comes into force at the time of its publication, unless it specifies a different time for its coming into force.

(5) In this section, "the 40-day period" means the period of 40 days beginning with the day on which the draft is laid before Parliament (or, if the draft is not laid before each House on the same day, the later of the days on which it is laid).

(6) In calculating the 40-day period, no account is to be taken of any period during which Parliament is dissolved or prorogued or during which both Houses of Parliament are adjourned for more than 4 days.

39 Effects of code of practice

(1) A failure by a regulated person to act in accordance with a provision of a code under section 37—
  (a) is not of itself evidence of a failure to comply with a requirement to which the provision of the code relates, and
  (b) does not of itself make the person liable to legal proceedings in a court or tribunal.

(2) A code under section 37 is admissible in evidence in legal proceedings.

(3) In any proceedings in a court or tribunal, the court or tribunal must take into account a provision of a code under section 37 in determining a question arising in the proceedings if—
  (a) the question relates to a time when the provision was in force, and
  (b) the provision appears to the court or tribunal to be relevant to the question.

(4) A regulatory authority must, when determining any question relating to a regulated person's compliance with a requirement imposed under or by virtue of regulations under section 29(1) or the NIS Regulations, take into account any provision of a code under section 37 if—

(a) the question relates to a time when the provision was in force, and
(b) the provision appears to the authority to be relevant to the question.

40 Withdrawal of code of practice

(1) The Secretary of State may withdraw a code issued under section 37.

(2) Before withdrawing a code, the Secretary of State must consult such persons as the Secretary of State considers appropriate on the proposal to withdraw the code.

(3) If the Secretary of State decides to withdraw a code, the Secretary of State must lay before Parliament notice of the withdrawal of the code.

(4) A withdrawal of a code has effect at the end of the 40-day period unless the notice under subsection (3) specifies that the withdrawal has effect at a different time; and a notice may specify different times for different purposes and may include savings.

(5) In subsection (4), "the 40-day period" has the same meaning as in section 38 (reading references in section 38(5) to a draft of the code as references to the notice).

CHAPTER 5

REPORT ON NETWORK AND INFORMATION SYSTEMS LEGISLATION

41 Report on network and information systems legislation

(1) The Secretary of State must at least once every 3 years beginning with the day on which this Act is passed—
(a) lay before Parliament a report on the operation of the legislation mentioned in subsection (3) during the review period, and
(b) publish the report.

(2) The review period means—
(a) in relation to the first report, the period between the day on which this Act is passed and the publication of the report;
(b) in relation to any other report, the period since the publication of the preceding report.

(3) The legislation referred to in subsection (1)(a) is such of the following legislation as has been in force at any time during the review period in question—
(a) the NIS Regulations;
(b) this Part and Part 4;
(c) regulations under any provision of Chapter 1 or 3 of this Part.

(4) A report must in particular—

(a) set out the objectives intended to be achieved by the legislation mentioned in subsection (3);
(b) assess the extent to which those objectives have been achieved;
(c) assess whether those objectives remain appropriate;
(d) if those objectives remain appropriate, assess the extent to which they could be achieved in another way which involves less onerous regulatory provision (as defined by section 32(4) of the Small Business, Enterprise and Employment Act 2015);
(e) review any exercise of the powers conferred on the Secretary of State by this Part and Part 4 during the review period in question.

(5) The Secretary of State may by regulations—
(a) specify matters that, in addition to those mentioned in subsection (4), must be covered in a report;
(b) impose requirements about the way in which a matter mentioned in subsection (4), or a matter specified by virtue of paragraph (a), is to be covered in a report.

(6) The Secretary of State may by notice given to a regulatory authority require the authority to provide such information as the Secretary of State may reasonably require for the purposes of a report.

CHAPTER 6

REGULATIONS UNDER PART 3

42 Regulations under section 24 or Chapter 3

(1) Regulations under section 24 or Chapter 3 may—
(a) make different provision for different purposes (including different provision for different descriptions of regulated person as defined by section 30(2));
(b) make provision subject to exceptions;
(c) make different provision for different areas;
(d) make provision about application to the Crown;
(e) make provision about application to relevant UK waters;
(f) make consequential, supplementary, incidental, transitional or saving provision.

(2) In subsection (1)(e), "relevant UK waters" means—
(a) internal waters of the United Kingdom,
(b) the territorial sea adjacent to the United Kingdom, and
(c) the sea (including the seabed and subsoil) in any area designated under section 1(7) of the Continental Shelf Act 1964.

(3) The consequential provision that may be made by virtue of subsection (1)(f) includes provision amending or repealing provision made by primary legislation.

(4) In subsection (3), "primary legislation" means—
  (a) an Act of Parliament (including this Act),
  (b) an Act of the Scottish Parliament,
  (c) an Act or Measure of Senedd Cymru, or
  (d) Northern Ireland legislation.

43 Consultation and procedure

(1) The Secretary of State must consult such persons as the Secretary of State considers appropriate before making—
  (a) regulations under section 24(3) (essential activities);
  (b) regulations under section 24(6) (designation of regulatory authorities);
  (c) regulations under section 29(1) which contain provision to which subsection (2) applies;
  (d) regulations under section 32(2)(a) or (b) (provision about meaning of "AI agent" and "loss of oversight or control");
  (e) regulations under section 41(5) (matters to be covered in reports on legislation).

(2) This subsection applies to provision made by virtue of any of the following—
  (a) section 30(1) (imposition of requirements on regulated persons), other than provision described in section 30(4) (designation of regulated persons);
  (b) section 31(1) (functions of regulatory authorities);
  (c) section 31(6) (appeals), other than provision described in section 31(7)(b) (procedure);
  (d) section 32(1) (functions of Secretary of State);
  (e) section 33(3) (maximum amount of penalties), other than where the provision is made for the purpose of reflecting inflation;
  (f) section 34(1)(a) or (2)(a) (disclosure of information), other than provision described in section 34(3)(b) (form of requirement to disclose information);
  (g) section 34(6) (functions of other persons);
  (h) section 35 (recovery of costs).

(3) The duty under subsection (1) may be satisfied by consultation carried out before the coming into force of this section.

(4) Regulations under this Part are to be made by statutory instrument.

(5) A statutory instrument containing regulations under this Part—
  (a) in relation to which consultation is required by subsection (1), or
  (b) which amend primary legislation as defined by section 42(4),

may not be made unless a draft of the instrument has been laid before and approved by a resolution of each House of Parliament.

(6) Any other statutory instrument containing regulations under this Part is subject to annulment in pursuance of a resolution of either House of Parliament.

PART 4

DIRECTIONS FOR NATIONAL SECURITY PURPOSES

CHAPTER 1

VENDOR-RELATED DIRECTIONS ETC

44 Vendor-related directions

(1) The Secretary of State may give a direction to a person ("P") if—

(a) P is specified or of a description specified for the purposes of this paragraph in regulations made by the Secretary of State by statutory instrument, and

(b) conditions 1 and 2 are met.

(2) A person may be specified in regulations under subsection (1)(a) only if the person, or every person of that description—

(a) is specified or of a description specified for the purposes of section 30(2),

(b) carries on a Part 4 essential activity in the United Kingdom, or

(c) provides essential goods or services.

(3) Condition 1 is that the Secretary of State considers that a risk to national security arises or could arise as a result of the use or potential use by P, in connection with a system that is a Part 4 NIS in relation to P, of goods, services or facilities provided by another person.

(4) Condition 2 is that the Secretary of State considers that—

(a) the direction is necessary having regard to that risk, and

(b) the requirements imposed by the direction are proportionate to what is sought to be achieved by the direction.

(5) A direction under this section is a direction requiring P to do, or not to do, a particular thing specified in the direction with a view to eliminating, reducing or mitigating the risk referred to in subsection (3).

(6) A direction under this section may in particular impose any of the following kinds of requirement—

(a) a requirement relating to the management of a system that is a Part 4 NIS in relation to P;

(b) a requirement designed to reduce risks relating to, or to mitigate impacts on, the carrying on of a Part 4 essential activity or the provision of essential goods or services;

(c) a requirement relating to the provision of information, including information relating to compliance with the direction;

(d) a requirement in the form of a prohibition or restriction on the use of goods, services or facilities;

(e) a requirement in the form of a prohibition on the installation of goods or the taking up of services or facilities;

(f) a requirement relating to removing, disabling or modifying goods or facilities or modifying services;

(g) a requirement for P to appoint a person with expertise in relation to the security of network and information systems (a "skilled person") for the purpose of assisting P to comply with the direction;

(h) a requirement for a thing to be done or not done in or in relation to the United Kingdom, relevant UK waters (as defined by section 42(2)) or a place other than the United Kingdom.

(7) Before making regulations under subsection (1)(a), the Secretary of State must consult such persons as the Secretary of State considers appropriate, so far as it is reasonably practicable to do so.

(8) Regulations under subsection (1)(a) may make different provision for different purposes.

(9) A statutory instrument containing regulations under subsection (1)(a) may not be made unless a draft of the instrument has been laid before and approved by a resolution of each House of Parliament.

45 Further provision about giving of vendor-related directions

(1) It does not matter for the purposes of section 44 whether or not—

(a) the risk referred to in section 44(3) relates to the carrying on of a Part 4 essential activity or the provision of essential goods or services;

(b) the person referred to in section 44(3) by whom goods, services or facilities are provided ("the vendor") is established in the United Kingdom;

(c) the goods, services or facilities provided by the vendor are provided from within or outside the United Kingdom;

(d) the use or proposed use of goods, services or facilities is or would be within the United Kingdom.

(2) A direction under section 44 must specify—

(a) the person to which the direction is given;

(b) the vendor to which the direction relates;

(c) the goods, services or facilities to which the direction relates;

(d) the reasons for the direction, except if or to the extent that the Secretary of State considers that it would be contrary to the interests of national security to do so;

(e) the time at which the direction comes into force;

(f) in relation to each requirement imposed by the direction that requires a thing to be done, a reasonable period within which the requirement must be complied with.

(3) A person to which a direction is given under section 44 must comply with it.

(4) A person to which a direction is given under section 44 ("P") –

(a) must obtain the written approval of the Secretary of State before appointing a skilled person for the purpose of assisting P to comply with the direction (whether or not in pursuance of a requirement imposed by virtue of section 44(6)(g));

(b) must notify the Secretary of State as soon as reasonably practicable after appointing a skilled person (whether or not in pursuance of such a requirement).

(5) For the purposes of giving approval as required by subsection (4)(a), the Secretary of State may rely on a list of persons published by the Government Communications Headquarters.

(6) Before giving a direction under section 44 to a person, the Secretary of State must consult –

(a) that person,

(b) the vendor to which the direction relates, and

(c) such other persons as the Secretary of State considers it appropriate to consult,

so far as it is reasonably practicable to do so.

(7) The duty under subsection (6) does not apply if or to the extent that the Secretary of State considers that compliance with the duty would be contrary to the interests of national security.

(8) The Secretary of State may require –

(a) a person to which a direction is given under section 44 not to disclose, in whole or part, the existence of the direction and the contents of the direction without the permission of the Secretary of State;

(b) a person consulted under subsection (6) not to disclose, in whole or part, the existence of the consultation and any information disclosed to the person in the consultation without the permission of the Secretary of State.

(9) The Secretary of State may not impose a requirement under subsection (8) unless the Secretary of State considers that the requirement is necessary and proportionate in the interests of national security.

46 Power to make regulations about time frame for giving vendor-related directions

(1) The Secretary of State may by regulations made by statutory instrument make provision about the time frame for determining whether to give a direction under section 44 (whether on a referral by a person specified or of a description specified for the purposes of subsection (1)(a) of that section or otherwise).

(2) The provision that may be made by regulations under subsection (1) includes, in particular, provision—

(a) about the period for making the decision;

(b) enabling the Secretary of State to extend or pause the period in circumstances specified or described in the regulations.

(3) Regulations under subsection (1) may—

(a) make different provision for different purposes;

(b) make provision subject to exceptions;

(c) make consequential, supplementary, incidental, transitional or saving provision;

(d) confer functions involving the exercise of a discretion.

(4) A statutory instrument containing regulations under subsection (1) is subject to annulment in pursuance of a resolution of either House of Parliament.

47 Power to establish mandatory referral scheme

(1) The Secretary of State may by regulations made by statutory instrument make provision for the establishment and operation of a mandatory referral scheme.

(2) A "mandatory referral scheme" is a scheme which, for the purpose of enabling the Secretary of State to determine whether to give a direction under section 44 in respect of a qualifying transaction, requires a person specified or of a description specified in regulations under section 44(1)(a) to refer the transaction to the Secretary of State.

(3) The Secretary of State may make regulations under this section establishing a mandatory referral scheme only if the Secretary of State considers that the establishment of such a scheme is necessary or expedient in the interests of national security.

(4) "Qualifying transaction" has the meaning given by regulations under this section.

(5) Provision made by virtue of subsection (4) may define "qualifying transaction" by reference to criteria set out in the regulations, which may, for example, be framed by reference to—

(a) the nature of a transaction,

(b) the value of a transaction,

(c) whether or not a transaction is critical to the carrying on of a Part 4 essential activity or the provision of essential goods or services, or

(d) the identity of the vendor in relation to a transaction.

(6) Regulations under this section may make provision about—

(a) when a person is required to make a referral;

(b) the procedure for making a referral;

(c) information to be provided in connection with a referral;

(d) monitoring of compliance with requirements imposed by the regulations;

(e) enforcement of compliance with requirements imposed by the regulations.

(7) The provision that may be made by virtue of subsection (6)(d) and (e) includes provision applying (with or without modifications) any provision made by sections 50 to 57.

(8) Before making regulations under this section, the Secretary of State must consult such persons as the Secretary of State considers appropriate, so far as it is reasonably practicable to do so.

(9) Regulations under this section may—

(a) make different provision for different purposes;

(b) make different provision for different areas;

(c) make provision subject to exceptions;

(d) require a person to have regard to guidance;

(e) make consequential, supplementary, incidental, transitional or saving provision.

(10) A statutory instrument containing regulations under this section may not be made unless a draft of the instrument has been laid before and approved by a resolution of each House of Parliament.

(11) References in this section to a transaction include references to a proposed transaction.

CHAPTER 2

GENERAL DIRECTIONS

48 General directions

(1) The Secretary of State may give a direction to a person within subsection (2) if the Secretary of State considers that—

(a) the occurrence of a security or operational compromise in relation to a system that is a Part 4 NIS in relation to the person, or the threat of such an occurrence, gives rise to a risk to national security, and

(b) the giving of the direction is necessary and proportionate in the interests of national security.

(2) A person is within this subsection if the person—

(a) is specified or of a description specified for the purposes of section 30(2), or

(b) is specified or of a description specified for the purposes of this paragraph in regulations made by the Secretary of State by statutory instrument.

(3) A person may be specified in regulations under subsection (2)(b) only if the person, or every person of that description—

(a) carries on a Part 4 essential activity in the United Kingdom, or

(b) provides essential goods or services.

(4) A direction under this section is a direction requiring the person to which it is given to do, or not to do, a particular thing specified in the direction with a view to eliminating, reducing or mitigating the risk referred to in subsection (1)(a).

(5) A direction under this section may in particular impose any of the following kinds of requirement—

(a) a requirement relating to the management of a system that is a Part 4 NIS in relation to the person to which the direction is given;

(b) a requirement designed to reduce risks relating to, or to mitigate impacts on, the carrying on of a Part 4 essential activity or the provision of essential goods or services;

(c) a requirement relating to the provision of information, including information relating to compliance with the direction;

(d) a requirement in the form of a prohibition or restriction on the use of goods, services or facilities;

(e) a requirement in the form of a prohibition on the installation of goods or the taking up of services or facilities;

(f) a requirement relating to removing, disabling or modifying goods or facilities or modifying services;

(g) a requirement for the person to which the direction is given ("P") to appoint a person with expertise in relation to the security of network and information systems (a "skilled person") for the purpose of assisting P to comply with the direction;

(h) a requirement for a thing to be done or not done in or in relation to the United Kingdom, relevant UK waters (as defined by section 42(2)) or a place other than the United Kingdom.

(6) Before making regulations under subsection (2)(b), the Secretary of State must consult such persons as the Secretary of State considers appropriate, so far as it is reasonably practicable to do so.

(7) It does not matter for the purposes of subsection (1) whether or not the risk referred to in subsection (1)(a) is one that relates to the carrying on of a Part 4 essential activity or the provision of essential goods or services.

(8) A direction under this section must specify—

(a) the person to which it is given;

(b) the reasons for the direction, except if or to the extent that the Secretary of State considers it would be contrary to the interests of national security to do so;

(c) the time at which the direction comes into force;

(d) in relation to each requirement imposed by the direction that requires a thing to be done, a reasonable period within which the requirement must be complied with.

(9) A person to which a direction is given under this section must comply with it.

(10) A person to which a direction is given under this section ("P")—

(a) must obtain the written approval of the Secretary of State before appointing a skilled person for the purpose of assisting P to comply with the direction (whether or not in pursuance of a requirement imposed by virtue of subsection (5)(g));

(b) must notify the Secretary of State as soon as reasonably practicable after appointing a skilled person (whether or not in pursuance of such a requirement).

(11) For the purposes of giving approval as required by subsection (10)(a), the Secretary of State may rely on a list of persons published by the Government Communications Headquarters.

(12) Before giving a direction under this section to a person, the Secretary of State must consult that person and such other persons as the Secretary of State considers appropriate, so far as it is reasonably practicable to do so.

(13) The duty under subsection (12) does not apply if or to the extent that the Secretary of State considers that compliance with the duty would be contrary to the interests of national security.

(14) The Secretary of State may require—

(a) a person to which a direction is given under this section not to disclose, in whole or part, the existence of the direction and the contents of the direction without the permission of the Secretary of State;

(b) a person consulted under subsection (12) not to disclose, in whole or part, the existence of the consultation and any information disclosed to the person in the consultation without the permission of the Secretary of State.

(15) The Secretary of State may not impose a requirement under subsection (14) unless the Secretary of State considers that the requirement is necessary and proportionate in the interests of national security.

(16) Regulations under subsection (2)(b) may make different provision for different purposes.

(17) A statutory instrument containing regulations under subsection (2)(b) may not be made unless a draft of the instrument has been laid before and approved by a resolution of each House of Parliament.

CHAPTER 3

DIRECTIONS UNDER SECTIONS 44 AND 48: SUPPLEMENTARY PROVISION

Compliance with directions to take priority

49 Compliance with directions under section 44 or 48 to take priority

(1) This section applies in a case where the Secretary of State—

(a) considers (following representations or otherwise) that it is not reasonably practicable for a person to which a relevant direction has been given to comply with both—

(i) a requirement imposed by a relevant direction given to the person, and

(ii) another requirement of a regulatory nature imposed under or by virtue of any enactment ("the conflicting requirement"), and

(b) has notified the person of that fact.

(2) In such a case, the person's duty to comply with the conflicting requirement does not apply so far as it conflicts with the requirement mentioned in subsection (1)(a)(i).

(3) The Secretary of State must notify any relevant regulator of the fact that the person is not required to comply with the conflicting requirement.

(4) "Relevant regulator" means a person which may exercise a regulatory function (within the meaning of the Legislative and Regulatory Reform Act 2006) in relation to—

(a) the person to which the relevant direction has been given, and

(b) the conflicting requirement.

(5) The duty under subsection (3) does not apply if or to the extent that the Secretary of State considers that compliance with the duty would be contrary to the interests of national security.

(6) Subsection (7) applies if under section 59 the Secretary of State—

(a) varies the relevant direction so as to remove the requirement mentioned in subsection (1)(a)(i), or

(b) revokes the relevant direction.

(7) In such a case—

(a) subsection (2) ceases to apply, and

(b) the Secretary of State must notify—

(i) the person to which the relevant direction has been given, and

(ii) any relevant regulator notified under subsection (3),

that subsection (2) has ceased to apply in relation to the conflicting requirement.

(8) In this section—

"enactment" includes an enactment comprised in, or in an instrument made under, an Act of the Scottish Parliament;

"relevant direction" means a direction under section 44 or 48.

Monitoring of compliance with directions

50 Monitoring by regulatory authorities

(1) The Secretary of State may direct a regulatory authority—

(a) to obtain information relating to a person's compliance with a direction given to the person under section 44 or 48,

(b) to prepare and send a report to the Secretary of State based on that information, and

(c) to provide to the Secretary of State on request the information on which a report falling within paragraph (b) is based.

(2) The information that the regulatory authority may be required to obtain under subsection (1)(a) is information which would assist the Secretary of State in determining whether the person has complied, is complying or is preparing to comply with the direction under section 44 or 48 or a particular requirement imposed by the direction.

(3) A regulatory authority to which a direction is given under this section must comply with it.

(4) A direction under this section may, in particular—

(a) require a report to include the regulatory authority's analysis of information gathered by the authority and an explanation of its analysis;

(b) make provision about the form and content of a report;

(c) require the authority to give the Secretary of State separate reports on different matters;

(d) make provision about when the authority must report to the Secretary of State, including provision requiring the authority to give reports at intervals specified in the direction.

(5) A regulatory authority to which a direction is given under this section must exercise its power under section 51(2) (information gathering) in such manner as it considers appropriate for the purposes of preparing a report required by the direction.

(6) The Secretary of State may vary or revoke a direction under this section.

(7) Before varying or revoking a direction under this section, the Secretary of State must consult the regulatory authority to which the direction was given.

(8) A direction may not be given under this section to a regulatory authority which is—

(a) a Minister of the Crown,

(b) a member of the Scottish Government or a junior Scottish Minister,

(c) the Welsh Government, or

(d) a Northern Ireland department.

(9) But subsection (8) does not prevent a regulatory authority referred to in that subsection from doing the things described in subsection (1) following a request made to the authority by the Secretary of State.

(10) The Secretary of State may disclose a report made by a regulatory authority in pursuance of subsection (1)(b) or (9).

(11) In disclosing such a report, the Secretary of State must have regard to the need to exclude from disclosure, so far as is practicable—

(a) information which relates to the affairs of a particular body and disclosure of which would or might, in the Secretary of State's opinion, seriously and prejudicially affect the interests of that body;

(b) information which relates to the private affairs of an individual and disclosure of which would or might, in the Secretary of State's opinion, seriously and prejudicially affect the interests of that individual.

Information gathering and inspections

51 Information gathering

(1) The Secretary of State may require a person to give the Secretary of State such information or documents as the Secretary of State reasonably requires for the purpose of exercising, or deciding whether to exercise, any of the Secretary of State's functions under this Part.

(2) A regulatory authority may require a regulated person to give the authority such information or documents as it reasonably requires for the purpose of complying with—

(a) a direction given to the authority under section 50, or

(b) a request of a kind referred to in section 50(9).

(3) A power under subsection (1) or (2) is to be exercised by giving the person in question a notice in writing (an "information notice").

(4) An information notice must—

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

(b) explain why the information or documents are being sought, except if or to the extent that the person giving the notice considers it would be contrary to the interests of national security to do so,

(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.

(5) A power under subsection (1) or (2) to require a person to give information includes the power to require the person—

(a) to obtain or generate information or documents;

(b) to collect or retain information or documents that the person would not otherwise collect or retain for the purpose of giving it under the subsection in question.

(6) A person to which an information notice is given must comply with the requirements imposed by the notice.

(7) The powers conferred by this section are exercisable in relation to information or documents whether stored within or outside the United Kingdom.

(8) A person may not be required by an information notice to give a privileged communication to the Secretary of State or a regulatory authority.

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

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

(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.

(10) An information notice given to a person ("P") may be revoked by notice given to P by the person which gave the information notice.

(11) In the application of this section 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.

(12) The power under subsection (1) may not be exercised in relation to—

(a) the person designated by regulation 4 of the NIS Regulations (single point of contact), or

(b) the person designated by regulation 5 of the NIS Regulations (computer security incident response team).

52 Inspections

(1) In this section—

"inspection" means any activity carried out for the purposes of or in connection with—

(a) verifying compliance with a direction under section 44 or 48 or a confirmation decision under section 55, or

(b) assessing or gathering evidence of a potential or alleged failure to comply with such a direction or decision;

"the affected person" means—

(a) where the inspection relates to a direction under section 44 or 48, the person to which the direction is given;

(b) where the inspection relates to a confirmation decision under section 55, the person to which the decision is given.

(2) The Secretary of State may—

(a) carry out all or any part of an inspection;

(b) appoint a person to carry out all or any part of an inspection on the Secretary of State's behalf (on such terms and in such a manner as the Secretary of State considers appropriate);

(c) direct the affected person to appoint a person who is approved by the Secretary of State to carry out all or any part of an inspection on the Secretary of State's behalf.

(3) Where a regulatory authority is subject to a direction under section 50 or a request has been made to it under section 50(9), it may—

(a) carry out all or any part of an inspection;

(b) appoint a person to carry out all or any part of an inspection on behalf of the authority (on such terms and in such a manner as the authority considers appropriate);

(c) direct the affected person to appoint a person who is approved by the authority to carry out all or any part of an inspection on its behalf.

(4) For the purposes of an inspection under subsection (2) or (3), the affected person must—

(a) pay the reasonable costs of the inspection if so required by the Secretary of State or regulatory authority (as the case may be);

(b) co-operate with the inspector;

(c) provide the inspector with access to their premises in accordance with subsection (6);

(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 subsection (8)(c);

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

(f) not intentionally obstruct an inspector performing their functions in relation to the carrying out of the inspection;

(g) comply with any request made by, or requirement of, an inspector in connection with the carrying out of an inspection.

(5) An inspector must, before carrying out all or part of an inspection under subsection (2) or (3), give the affected person a notice setting out information about the possible consequences of failure to comply with the duties imposed by subsection (4).

(6) An inspector may at any reasonable time enter the premises of the affected person, except any premises used wholly or mainly as a private dwelling, if

the inspector has reasonable grounds to believe that entry to the premises may be expedient for the purposes of the inspection.

(7) Before entering any premises under this section, the inspector must—

(a) produce evidence of their identity, and

(b) outline the purpose for which the power is exercised,

if asked to do so by a person on the premises.

(8) On entering any premises under this section, an inspector may (for the purposes of the inspection)—

(a) require the affected person to maintain (without alteration) any material, document, information or equipment found on the premises or accessible from the premises;

(b) require the affected person to produce and provide the inspector with access to any material, document, information or equipment;

(c) 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);

(d) interview any person;

(e) carry out, or direct the affected person to carry out, a test relating to the security of a network and information system, including a component of the system or a process connected with the system;

(f) take such other action as the inspector considers appropriate.

(9) A person may not be required under this section to produce, or provide an inspector with access to, a privileged communication (within the meaning given by section 51(9)).

(10) The powers conferred by this section—

(a) are not exercisable in relation to premises, material, equipment or individuals outside the United Kingdom;

(b) are exercisable in relation to documents or information whether stored within or outside the United Kingdom.

(11) In this section, "inspector" means a person carrying out all or any part of an inspection in accordance with this section.

Enforcement of requirements

53 Notification of contravention

(1) Where an enforcement authority determines that there are reasonable grounds for believing that a person is contravening or has contravened a relevant requirement, the authority may give the person a notification under this section.

(2) In this section and sections 54 to 56—

(a) "relevant requirement" means a requirement imposed—

(i) by a direction under section 44 or 48,

(ii) by section 45(4)(a) or 48(10)(a) (approval of skilled persons),

(iii) under section 51(1) or (2) (requirement to give information), or

(iv) under or by virtue of section 52(2)(c), (3)(c) or (4) (requirement relating to an inspection);

(b) "enforcement authority"—

(i) in relation to a relevant requirement within paragraph (a)(i) or (ii), means the Secretary of State;

(ii) in relation to any other relevant requirement, means the person which imposed the requirement.

(3) A notification under this section is one which—

(a) sets out the enforcement authority's determination,

(b) specifies the requirement and contravention in respect of which the determination is made,

(c) specifies the period during which the person to which the notification is given has an opportunity to make representations,

(d) specifies the steps which the enforcement authority thinks should be taken by that person in order to—

(i) comply with the requirement, and

(ii) remedy the consequences of the contravention, and

(e) specifies the penalty which the enforcement authority is minded to impose.

(4) A notification may be given in respect of more than one contravention; and, where such a notification is given, a separate penalty may be specified under subsection (3)(e) in respect of each contravention.

(5) If a notification is given in respect of a continuing contravention—

(a) it may be given in respect of any period during which the contravention has continued;

(b) no more than one penalty may be specified under subsection (3)(e) in respect of the period of contravention specified in the notification.

(6) Notwithstanding subsection (5)(b), in relation to a continuing contravention, a penalty may be specified in respect of each day on which the contravention continues after—

(a) the giving of a confirmation decision under section 55 which requires immediate action in respect of that contravention (see section 55(5)(a)), or

(b) the expiry of any period specified in the confirmation decision for complying with the requirement being contravened.

(7) Where a notification has been given to a person in respect of a contravention of a requirement, an enforcement authority may only give a further notification in respect of the same contravention if—

(a) the contravention is a continuing contravention and the subsequent notification is in respect of so much of a period as falls after a period to which the earlier notification relates, or

(b) the earlier notification has been withdrawn without a penalty having been imposed in respect of the notified contravention.

(8) It is immaterial for the purposes of this section whether conduct that constitutes or causes a contravention of a relevant requirement occurs inside the United Kingdom or elsewhere.

(9) If the condition in subsection (10) is met, an enforcement authority may require a person subject to a notification under this section not to disclose to any other person the existence or contents of—

(a) the notification, or

(b) a part of the notification specified by the authority,

without the permission of the authority.

(10) The condition is that the Secretary of State considers that it would be contrary to the interests of national security for the existence or contents of the whole or specified part of the notification to be disclosed.

54 Penalty amounts

(1) The amount of a penalty that may be specified in a notification under section 53 is such amount as the enforcement authority determines to be—

(a) appropriate, and

(b) proportionate to the contravention in respect of which it is imposed.

(2) The amount of a penalty may not exceed—

(a) in the case of a contravention of a requirement imposed by a direction under section 44 or 48 or by section 45(4)(a) or 48(10)(a) by a person which is an undertaking—

(i) £17,000,000, or

(ii) where regulations under subsection (5) are in force, the greater of—

(A) £17,000,000, and

(B) 10% of the turnover of the undertaking (both inside and outside the United Kingdom);

(b) in the case of a contravention of a requirement referred to in paragraph (a) by a person which is not an undertaking, £17,000,000;

(c) in the case of a contravention by a person of a requirement to give information under section 51(1) or (2) or of a requirement relating to an inspection imposed under or by virtue of section 52(2)(c), (3)(c) or (4), £10,000,000.

(3) In the case of a penalty specified under section 53(6), the amount may not exceed (subject to subsection (2))—

(a) in the case of a contravention of a requirement imposed by a direction under section 44 or 48 or by section 45(4)(a) or 48(10)(a), £100,000 per day;

(b) in the case of a contravention by a person of a requirement to give information under section 51(1) or (2) or of a requirement relating to an inspection imposed under or by virtue of section 52(2)(c), (3)(c) or (4), £50,000 per day.

(4) In imposing a penalty by reference to a daily rate—

(a) no account is to be taken of any days before the giving of the notification under section 53, and

(b) unless the enforcement authority determines an earlier day (whether before or after the penalty is imposed), the amount payable ceases to accumulate at the beginning of the day on which the person first complies with the requirement in question.

(5) The Secretary of State must by regulations made by statutory instrument make provision for the purposes of this section—

(a) about the meaning of "undertaking";

(b) about how an undertaking's turnover is to be determined.

(6) Regulations under subsection (5) may, in particular—

(a) include provision that a person of a description specified in the regulations is or is not an undertaking;

(b) make provision about amounts which are, or are not, to be taken into account in determining an undertaking's turnover;

(c) make provision about the period by reference to which an undertaking's turnover is to be determined;

(d) make provision conferring a power on the Secretary of State to make a determination in a particular case in relation to matters mentioned in the regulations (including the matters mentioned in paragraphs (b) and (c));

(e) provide, in a case where an undertaking is a member of a group, for other members of the group to be treated as part of the undertaking for the purposes of determining the undertaking's turnover;

(f) provide, in a case where an undertaking controls or is controlled by another person, for that person to be treated as part of the undertaking for the purposes of determining the undertaking's turnover,

and references in paragraph (f) to control are to be construed in accordance with the regulations.

(7) The Secretary of State may by regulations made by statutory instrument amend an amount for the time being specified in subsection (2)(a)(i) or (ii)(A), (b) or (c) or (3) for the purpose of reflecting inflation.

(8) Regulations under subsection (5) or (7) may—

(a) make different provision for different purposes;

(b) make different provision for different areas;

(c) make consequential, supplementary, incidental, transitional or saving provision.

(9) A statutory instrument containing regulations under subsection (5) or (7) is subject to annulment in pursuance of a resolution of either House of Parliament.

55 Enforcement of notification

(1) This section applies where—

(a) a person is given a notification by an enforcement authority under section 53, and

(b) the period allowed for the making of representations about the matters specified in the notification has expired.

(2) The enforcement authority may—

(a) give the person a decision ("a confirmation decision") confirming the imposition of requirements on the person in accordance with the notification, or

(b) inform the person that no further action will be taken.

(3) The enforcement authority may not give the person a confirmation decision unless, after considering any representations, the authority is satisfied that the person has, in one or more of the ways specified in the notification under section 53, contravened a relevant requirement specified in that notification.

(4) A confirmation decision must be given to the person without delay and include reasons for the decision.

(5) A confirmation decision may—

(a) require immediate action by the person—

(i) to comply with the relevant requirement specified in the notification under section 53, and

(ii) to remedy the consequences of the contravention, or

(b) specify a period within which the person must comply with that requirement and remedy those consequences,

and may specify the steps to be taken by the person in order to comply with that requirement or remedy those consequences.

(6) A confirmation decision may require the person to pay—

(a) the penalty specified in the notification under section 53, or

(b) such lesser penalty as the enforcement authority considers appropriate having regard to—

(i) any representations made by the person, and

(ii) any steps taken by the person to comply with the relevant requirement specified in the notification or to remedy the consequences of the contravention,

and may specify the period within which the penalty is to be paid.

(7) A person to which a confirmation decision is given must comply with any requirement imposed by the decision.

(8) The enforcement authority may enforce the duty imposed by subsection (7) in civil proceedings—

(a) for an injunction;

(b) for specific performance of a statutory duty under section 45 of the Court of Session Act 1988;

(c) for any other appropriate remedy or relief.

(9) If the condition in subsection (10) is met, an enforcement authority may require a person to which a confirmation decision has been given not to disclose the existence or contents of—

(a) the decision, or

(b) a part of the decision specified by the authority,

without the permission of the authority.

(10) The condition is that the Secretary of State considers that it would be contrary to the interests of national security for the existence or contents of the whole or specified part of the decision to be disclosed.

56 Enforcement of penalty

(1) This section applies where a sum is payable to an enforcement authority as a penalty under section 55.

(2) The penalty—

(a) is recoverable in England and Wales as if it were payable under an order of the county court;

(b) may be enforced in Scotland in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland;

(c) is recoverable in Northern Ireland as if it were payable under an order of a county court in Northern Ireland.

(3) Where action is taken under this section for the recovery of a sum payable as a penalty under section 55, the penalty is—

(a) in relation to England and Wales, to be treated for the purposes of section 98 of the Courts Act 2003 (register of judgments and orders 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 (S.I. 1981/226 (N.I. 6)) (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.

57 Enforcement of non-disclosure requirements

(1) In this section "non-disclosure requirement" means a requirement imposed under section 45(8), 48(14), 53(9) or 55(9).

(2) Where a person ("P") is required not to disclose a matter by a non-disclosure requirement, disclosure of that matter by an employee of P or a person engaged in P's business is to be regarded as a disclosure by P, unless P can show that they took all reasonable steps to prevent such a disclosure.

(3) Sections 53 to 56 apply in relation to a contravention of a non-disclosure requirement with the following modifications.

(4) Section 53 has effect as if—

(a) in subsection (1) for "relevant requirement" there were substituted "non-disclosure requirement";

(b) for subsection (2) there were substituted—

"(2) In this section and sections 54 to 56 "enforcement authority", in relation to a non-disclosure requirement, means the person which imposed the requirement.";

(c) for subsection (3)(d) there were substituted—

"(d) specifies the steps that the enforcement authority thinks should be taken by that person in order to—

(i) bring the contravention to an end, and

(ii) limit the consequences of the contravention, and";

(d) in subsection (8) for "relevant requirement" there were substituted "non-disclosure requirement".

(5) Section 54 has effect as if—

(a) for subsections (2) and (3) there were substituted—

"(2) The amount of a penalty may not exceed £10,000,000.

(3) In the case of a penalty specified under section 53(6), the amount may not exceed (subject to subsection (2)) £50,000 per day.";

(b) subsections (5) to (9) were omitted.

(6) Section 55 has effect as if—

(a) in subsection (3) for "relevant requirement" there were substituted "non-disclosure requirement";

(b) for subsection (5) there were substituted—

"(5) A confirmation decision may—

(a) require immediate action by the person—

(i) to bring the contravention to an end, and

(ii) to limit the consequences of the contravention, or

(b) specify a period within which the person must bring that contravention to an end and limit those consequences,

and may specify the steps to be taken by the person in order to bring that contravention to an end or limit those consequences.";

(c) for subsection (6)(b)(ii) there were substituted—

"(ii) any steps taken by the person to bring the contravention to an end or to limit the consequences of the contravention,".

CHAPTER 4

DIRECTIONS TO REGULATORY AUTHORITIES

58 Power to direct regulatory authorities

(1) The Secretary of State may give a direction to a regulatory authority as to the exercise by the authority of—

(a) its functions generally under the NIS Regulations, regulations under section 29(1) or this Part, or

(b) any of those functions specifically.

(2) The Secretary of State may give a direction under this section only if the Secretary of State considers that the giving of the direction is necessary and proportionate in the interests of national security.

(3) A direction under this section may require the regulatory authority to which it is given to provide information to a person specified in the direction about how the authority proposes to comply or has complied with the direction.

(4) A direction under this section must specify—

(a) the regulatory authority to which it is given,

(b) the reasons for the direction, except if or to the extent that the Secretary of State considers it would be contrary to the interests of national security to do so,

(c) the time at which the direction comes into force, and

(d) in relation to each requirement imposed by the direction that requires a thing to be done, a reasonable period within which the requirement is to be complied with.

(5) A regulatory authority to which a direction is given under this section must comply with it.

(6) A direction under this section may not be given to a regulatory authority which is—

(a) a Minister of the Crown,

(b) a member of the Scottish Government or a junior Scottish Minister,

(c) the Welsh Government, or

(d) a Northern Ireland department.

CHAPTER 5

GENERAL PROVISION

59 Review, variation and revocation of directions

(1) This section applies in relation to a direction given under section 44, 48 or 58.

(2) The Secretary of State—
  (a) must review the direction from time to time;
  (b) may vary or revoke the direction.

(3) The Secretary of State may vary the direction only if the Secretary of State considers that the direction as varied would be necessary and proportionate in the interests of national security.

(4) If the direction is varied, the Secretary of State must give notice of the variation to the person to which the direction was given.

(5) A notice under subsection (4) must specify—
  (a) how the direction is varied,
  (b) the reasons for the variation, except if or to the extent that the Secretary of State considers it would be contrary to the interests of national security to do so, and
  (c) the time at which the variation comes into force.

(6) If the direction is revoked, the Secretary of State must give notice of the revocation to the person to which the direction was given, which must specify the time at which the revocation comes into force.

(7) Before varying a direction given to a person under section 44 or 48, the Secretary of State must consult that person and such other persons as the Secretary of State considers appropriate, so far as it is reasonably practicable to do so.

(8) The duty under subsection (7) does not apply if or to the extent that the Secretary of State considers that compliance with the duty would be contrary to the interests of national security.

(9) If the condition in subsection (10) is met, the Secretary of State may require a person consulted under subsection (7) not to disclose—
  (a) the existence of the consultation, or
  (b) the whole or part of any information disclosed to the person in the course of the consultation,

without the permission of the Secretary of State.

(10) The condition is that the Secretary of State considers that it would be contrary to the interests of national security for the existence of the consultation, or the information in question, to be disclosed.

(11) Section 57 applies in relation to a requirement imposed under subsection (9) as if it were a non-disclosure requirement within the meaning of that section.

60 Publication of notice of direction under section 44 etc

(1) Subject to subsection (3), the Secretary of State must publish, in such manner as the Secretary of State considers appropriate, notice of the fact that—

(a) a direction under section 44 has been given, or

(b) such a direction has been varied or revoked under section 59.

(2) The notice under subsection (1) must be published as soon as practicable and must—

(a) state when the direction, variation or revocation comes into force,

(b) state the person to which the direction, variation or revocation has been given,

(c) include a summary of the direction, variation or revocation, its effect and the reasons for it, and

(d) include any other information that the Secretary of State considers it appropriate to include.

(3) The Secretary of State may exclude from the notice under subsection (1) anything the publication of which the Secretary of State considers—

(a) might harm the commercial interests of any person to an unreasonable degree, or

(b) would be contrary to the interests of national security.

61 Annual report in relation to directions under section 44

(1) The Secretary of State must, in relation to each relevant period—

(a) prepare a report in accordance with this section, and

(b) lay a copy of it before Parliament as soon as practicable after the end of that period.

(2) Each report must provide details of—

(a) the number of directions given under section 44 during the relevant period,

(b) the kinds of services provided by persons to which directions under section 44 were given during the relevant period (including, where relevant, the sectors in which the services are provided),

(c) the number of directions under section 44 that have been varied during the relevant period, and

(d) the number of directions under section 44 that have been revoked during the relevant period.

(3) "Relevant period" means—

(a) the period of 12 months beginning with the day on which section 44(1) comes into force for any purpose other than the purpose of making regulations;

(b) each subsequent period of 12 months.

62 Laying before Parliament: directions under sections 48 and 58 etc

(1) The Secretary of State must lay before Parliament a copy of—

(a) a direction given under section 48;

(b) a direction given under section 58;

(c) a notice of variation given under section 59 in respect of a direction under section 48 or 58.

(2) Subsection (1) does not apply if the Secretary of State considers that laying a copy of the direction or notice before Parliament would be contrary to the interests of national security.

(3) The Secretary of State may exclude from what is laid before Parliament anything the publication of which the Secretary of State considers—

(a) might harm the commercial interests of any person to an unreasonable degree, or

(b) would be contrary to the interests of national security.

63 Information sharing

(1) The Secretary of State may disclose information obtained by the Secretary of State under this Part to—

(a) a regulatory authority,

(b) the Government Communications Headquarters,

(c) a UK public authority which does not fall within paragraph (a) or (b), or

(d) an overseas public authority.

(2) A regulatory authority may disclose information obtained by the authority under this Part to—

(a) the Secretary of State,

(b) another regulatory authority,

(c) the Government Communications Headquarters,

(d) a UK public authority which does not fall within paragraph (a), (b) or (c), or

(e) an overseas public authority.

(3) A disclosure of information under this section must be—

(a) necessary for national security purposes, and

(b) limited to information which is relevant and proportionate to the purpose for which the disclosure is made.

(4) Except as provided by subsection (5), the disclosure of information under this section 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).

(5) This section does not authorise a disclosure of information if the disclosure is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.

(6) In this section—

"overseas public authority" means a person in any country or territory outside the United Kingdom which appears to the person proposing to disclose information to exercise functions of a public nature which—

(a) correspond to functions under this Part or under the NIS Regulations of—

(i) the Secretary of State, or

(ii) a regulatory authority, or

(b) relate to national security;

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

64 Means of giving directions, notices etc

(1) A direction, notice, notification or decision under this Part may be given to a person by—

(a) delivering it by hand to a relevant individual,

(b) leaving it at the person's proper address,

(c) sending it by post to the person at that address, or

(d) sending it by email to the person's email address.

(2) Where a regulated person has—

(a) appointed a representative to act on their behalf, and

(b) notified a regulatory authority of the appointment,

a direction, notice, notification or decision under this Part may be given to that representative instead of the regulated person, by any of the methods mentioned in subsection (1).

(3) Any direction, notice, notification or decision given to a representative by virtue of subsection (2) is to be treated as having been given to the regulated person.

(4) A "relevant individual" means—

(a) in the case of a direction, notice, notification or decision given to an individual, that individual;

(b) in the case of a direction, notice, notification or decision given to a body corporate (other than a partnership), an officer of that body;

(c) in the case of a direction, notice, notification or decision given to a partnership (including a Scottish partnership), a partner in the partnership or a person who has the control or management of the partnership business;

(d) in the case of a direction, notice, notification or decision given to an unincorporated body (other than a partnership), a member of its governing body.

(5) For the purposes of subsection (1)(b) and (c), and section 7 of the Interpretation Act 1978 (service of documents by post) in its application to those provisions, a person's proper address is—

(a) in a case where the person has specified an address as one at which the person, or someone acting on the person's behalf, will accept service of notices or other documents, that address;

(b) in any other case, the address determined in accordance with subsection (6).

(6) The address is—

(a) in a case where the person is a body corporate with a registered office in the United Kingdom, that office;

(b) in a case where paragraph (a) does not apply and the person is a body corporate, partnership or unincorporated body with a principal office in the United Kingdom, that office;

(c) in any other case, an address in the United Kingdom at which the person giving the direction, notice, notification or decision believes, on reasonable grounds, that it will come to the attention of the person to whom it is to be given.

(7) A person's email address is—

(a) an email address provided to a regulatory authority as an address for contacting that person,

(b) an email address published for the time being by that person as an address for contacting that person, or

(c) if no email address has been so provided or published, an email address by means of which the person giving the direction, notice, notification or decision believes, on reasonable grounds, that it will come to the attention of that person.

(8) A direction, notice, notification or decision sent to a person by email is, unless the contrary is proved, to be treated as having been given at 9am on the working day immediately following the day on which it was sent.

(9) In subsection (8) "working day" means a day other than a Saturday, a Sunday, Christmas Day, Good Friday or a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom.

(10) In this section "officer", in relation to a body corporate, means a director, manager, secretary or other similar officer of the body.

65 Interpretation of Part 4

(1) In this Part—

"essential goods or services" means goods or services without the provision of which the carrying on of a Part 4 essential activity would be at risk of disruption;

"Minister of the Crown" has the same meaning as in the Ministers of the Crown Act 1975 (see section 8(1) of that Act);

"network and information system" has the same meaning as in Part 3;

"Part 4 essential activity" means an activity the carrying on of which the Secretary of State considers to be essential to—

(a) the economy of the United Kingdom or any part of the United Kingdom, or

(b) the day-to-day functioning of society in the United Kingdom or any part of the United Kingdom;

"Part 4 NIS", in relation to a person, means a network and information system that is—

(a) used or relied on by the person in connection with the carrying on of a Part 4 essential activity or the provision of essential goods or services, or

(b) associated with a system mentioned in paragraph (a) (and section 29(4) (meaning of "associated") applies for the purposes of this paragraph as it applies for the purposes of section 29(3));

"regulated person" has the same meaning as in Chapter 3 of Part 3 (see section 30(2) and (5));

"regulatory authority" means a person designated for the purposes of section 24(6) (and includes the persons treated by section 24(8) as having been so designated);

"security or operational compromise", in relation to a network and information system, means—

(a) anything that compromises the security, availability, functionality or reliability of the system,

(b) any unauthorised access to, interference with or exploitation of the system or anything which enables such access, interference or exploitation,

(c) anything that compromises the confidentiality, authenticity, integrity or availability of data stored on or processed, received or transmitted by the system, or

(d) anything that causes data stored on or processed by the system to be lost.

(2) For the purposes of this Part—

(a) a reference to the carrying on of an activity includes a reference to the provision of a service;

(b) a reference to a person specified or of a description specified for the purposes of section 30(2) includes a reference to a person treated by section 30(5) as having been so specified.

66 Review of the effectiveness of the NIS regime

(1) The Secretary of State must, within 12 months of the day on which this Act is passed, carry out a review of the effectiveness of this Act and the NIS Regulations in securing the security and resilience of the network and information systems on which the economy and the day-to-day functioning of society in the United Kingdom depend.

(2) In particular, the review must, in the context of the regulatory system established by this Act and the NIS Regulations—

(a) identify the categories of organisation, in both the public and private sectors, that have a material impact on the economy, society or national defence and security, and identify what obligations could be placed upon them to improve their cyber resilience,

(b) review the critical vulnerabilities of technology platforms and identify what obligations could be placed on technology providers to supply safe services, and to address vulnerabilities when they occur, and

(c) review the options for regulating organisations and technology providers to promote cyber resilience.

(3) The review must consider—

(a) the sectors and activities currently within scope;

(b) the management of supply chain risks;

(c) whether further sectors and activities should be specified as essential activities under section 24(3), or otherwise brought within the scope of the NIS Regulations, having particular regard to—

(i) all sectors forming part of the United Kingdom's critical national infrastructure,

(ii) digital infrastructure, including cloud services, software-as-a-service, and content delivery networks,

(iii) frontier artificial intelligence models and systems, or other frontier agentic technologies,

(iv) democratic processes, including election administration and registered political parties,

(v) advanced manufacturing, life sciences, and critical transport equipment, and

(vi) sectors of social importance, including education, research organisations, and large-scale retail distribution of essential goods other than food;

(d) the institutional and regulatory framework established or otherwise affected by this Act and the NIS Regulations, including the roles and powers of the Secretary of State, designated competent authorities, the National Cyber Security Centre, the Information Commissioner, and the AI Security Institute.

(4) In considering the sectors and activities currently within scope, the Secretary of State must assess—

(a) whether essential activities are appropriately defined and effectively regulated,

(b) whether the thresholds for regulation under the NIS Regulations, including those which exclude micro and small enterprises, leave significant risks unaddressed, and

(c) how effectively risks arising in supply chains are managed.

(5) In considering the regulatory system established or otherwise affected by this Act and the NIS Regulations, the Secretary of State must consider—

(a) the institutional framework for the exercise of functions under this Act and the NIS Regulations, including the roles and powers of the Secretary of State, the designated competent authorities, the National Cyber Security Centre and the Information Commission, and whether that framework is the optimum framework for promoting cyber resilience across the United Kingdom,

(b) the obligations to promote cyber resilience placed on—

(i) persons within scope of the NIS Regulations,

(ii) other organisations and sectors which could facilitate or contribute to security or operational compromises of relevant network and information systems,

(iii) the developers of emerging and frontier technologies which could compromise relevant network and information systems, and

(iv) organisations and sectors making a material impact on the economy, society, defence or security of the United Kingdom,

(c) the powers of the AI Security Institute in relation to frontier AI systems that pose a material risk to the security or resilience of network and information systems used in essential activities—

(i) to audit such systems before they are deployed or made available for use in such network and information systems,

(ii) to set and review safety standards for such systems,

(iii) to inspect such systems and the practices of their developers and deployers, and

(iv) to require remedial action, including the suspension or restriction of the provision or deployment of a system, or to recommend that the Secretary of State do so,

(d) whether the supply of cyber security professionals required to ensure security or resilience of network and information systems used in essential activities is sufficient, and

(e) the obligations placed on regulated persons to report notifications of incidents, including whether the timelines and notifications are sufficient.

(6) In carrying out the review, the Secretary of State must have regard to—

(a) the impact that an incident affecting network and information systems relied on in the carrying on of an activity would be likely to have on

the economy or the day-to-day functioning of society in the United Kingdom or any part of it,

(b) the role of persons carrying on the activity in the supply of essential goods and services and in supply chains,

(c) the extent to which the activity is already subject to comparable requirements relating to the security and resilience of network and information systems, and

(d) the need for regulation to be proportionate, evidence-based and transparent.

(7) In carrying out the review, the Secretary of State must consult—

(a) the National Cyber Security Centre,

(b) the Information Commission,

(c) the designated competent authorities,

(d) the AI Security Institute, and

(e) such other persons as the Secretary of State considers appropriate.

(8) On completing the review, the Secretary of State must lay before Parliament a report setting out—

(a) the findings of the review on each of the matters mentioned in subsections (2) and (3),

(b) the activities (if any) which the Secretary of State intends to specify as essential activities, or otherwise to bring within the scope of the NIS Regulations, and the timetable for doing so,

(c) the reasons for not bringing within scope any activity mentioned in subsection (4) or (5) which the Secretary of State does not intend to bring within scope, and

(d) the changes (if any) which the Secretary of State intends to make to the regulatory system, and the timetable for doing so.

(9) Where a report under subsection (8) concludes that an activity should be brought within the scope of the NIS Regulations or of regulations under section 29(1), the Secretary of State must, within six months of the report being laid—

(a) lay before Parliament a draft of regulations under section 24(3) specifying that activity, or

(b) lay before Parliament a statement explaining why the Secretary of State does not intend to do so.

(10) The Secretary of State must, at intervals of not more than 12 months after the report under subsection (8) is laid, carry out a further review in accordance with subsections (1) to (7) and lay before Parliament a report on that review setting out the matters mentioned in subsection (8).

(11) In this section—

"frontier AI system" means a highly capable general-purpose artificial intelligence model or system that can perform a wide variety of tasks

and matches or exceeds the capabilities of the most advanced contemporary models;

"frontier agentic technology" means any machine-based system which, for explicit or implicit objectives, infers from the input it receives how to generate outputs that can influence physical or virtual environments, and which—

(a) can act autonomously, taking sequences of actions without human direction, and can adaptably achieve complex goals in complex environments with limited direct human supervision, and

(b) has capabilities which match or exceed those present in the most advanced AI models or systems at the time.

67 Register of foreign powers for the purposes of Part 4

(1) For the purposes of informing action taken under Part 4 of this Act, the Secretary of State must, by regulations made by statutory instrument, and within six months of the day on which this Act is passed, establish and maintain a register of foreign powers that the Secretary of State believes present a risk to the United Kingdom's critical network and information systems.

(2) Foreign powers designated by the Secretary of State under subsection (1) must include states—

(a) which have been confirmed by GCHQ as having—

(i) perpetrated, or attempted to perpetrate, a cyber attack in the UK in the preceding seven years,

(ii) targeted, or intended to target, that attack at the network or information systems of one or more operators of an essential service or critical suppliers, and

(iii) carried out, or intended to carry out, that attack through a state department, agency or affiliate group;

(b) which GCHQ has warned pose a risk to the security or resilience of the network or information systems of one or more operators of an essential service or critical suppliers.

(3) For each foreign power added to the register established under subsection (1), the Secretary of State must review the extent and nature of the risk posed to the network and information systems of operators of essential services and critical suppliers, including whether the risk arises from—

(a) activities undertaken outside of the UK, or

(b) foreign owned or controlled infrastructure or locations within the UK.

(4) Within six months of the establishment of the register under subsection (1), the Secretary of State must lay before Parliament a report containing—

(a) the findings and conclusions of the review conducted under subsection (3), and

(b) the Government's plan for addressing the risks identified.

(5) If the Secretary of State considers that laying a report, or any portion of a report, under subsection (4) would be contrary to the interests of national security, the Secretary of State must make a statement to Parliament confirming that—

(a) a review has been conducted under subsection (3), and

(b) that the report, or a portion of the report, cannot be laid before Parliament for reasons of national security.

(6) A statutory instrument containing regulations under this section may not be made unless a draft of the instrument has been laid before, and approved by a resolution of, each House of Parliament.

(7) In this section, "foreign power" means—

(a) the sovereign or other head of a foreign state in their public capacity,

(b) a foreign government, or part of a foreign government,

(c) an agency or authority of a foreign government, or of part of a foreign government,

(d) an authority responsible for administering the affairs of an area within a foreign country or territory, or persons exercising the functions of such an authority, or

(e) a political party which is a governing political party of a foreign government.

(8) A political party is a governing political party of a foreign government if persons holding political or official posts in the foreign government or part of the foreign government—

(a) hold those posts as a result of, or in the course of, their membership of the party, or

(b) in exercising the functions of those posts, are subject to the direction or control of, or significantly influenced by, the party.

PART 5

GENERAL

68 Extent

This Act extends to England and Wales, Scotland and Northern Ireland.

69 Commencement

(1) The following come into force on the day on which this Act is passed—

(a) Part 1;

(b) Chapters 1, 3 and 6 of Part 3;

(c) section 41;

(d) this Part.

(2) The following come into force two months after the day on which this Act is passed—

(a) section 18(3) and (4);

(b) Chapter 2 of Part 3;

(c) paragraphs 3, 4 and 15 of Schedule 2.

(3) The other provisions of this Act come into force on such day as the Secretary of State may appoint by regulations.

(4) Regulations under subsection (3) may appoint different days for different purposes.

(5) Regulations under subsection (3) may not appoint a day for the coming into force of section 12 (critical suppliers) which is different from the day on which the first regulations under section 29(1) which contain relevant amending provision come into force so far as relating to that provision.

(6) In subsection (5), "relevant amending provision" means provision amending the NIS Regulations so as to impose requirements on providers of activity-critical supplies (within the meaning of Chapter 3 of Part 3).

(7) The Secretary of State may by regulations make transitional or saving provision in connection with the coming into force of any provision of this Act.

(8) Regulations under subsection (7) may make different provision for different purposes.

(9) Regulations under this section are to be made by statutory instrument.

70 Short title

(1) This Act may be cited as the Cyber Security and Resilience (Network and Information Systems) Act 2026.

SCHEDULES

SCHEDULE 1

Section 22

ENFORCEMENT AND APPEALS

1 The NIS Regulations are amended as follows.

2 (1) Regulation 16 (power of inspection) is amended as follows.

(2) In paragraph (2)(c), after "RDSP" insert "or RMSP".

(3) In paragraph (3), for "or RDSP" substitute ", RDSP or RMSP".

(4) After paragraph (4) insert—

"(4A) An inspector must, before conducting all or any part of an inspection under paragraph (1) or (2), give the OES, RDSP or RMSP (as the case may be) a notice setting out information about the possible consequences of failure to comply with the duties imposed by paragraph (3)."

(5) In paragraph (5), in each of sub-paragraphs (a), (b), (c) and (f), for "or RDSP" substitute ", RDSP or RMSP".

(6) In paragraph (7)(a), for "or RDSP" substitute ", RDSP or RMSP".

(7) After paragraph (8) insert—

"(8A) A person may not be required under this regulation to produce, or provide an inspector with access to, a privileged communication.

(8B) The powers conferred by this regulation—

(a) are not exercisable in relation to premises, material, equipment or individuals outside the United Kingdom;

(b) are exercisable in relation to documents or information whether stored within or outside the United Kingdom."

(8) In paragraph (9), at the end insert—

"(d) "privileged communication" has the meaning given by regulation 15A(5)."

3 (1) Regulation 17 (enforcement notices for breach of duties) is amended as follows.

(2) In paragraph (1)—

(a) after sub-paragraph (za) insert—

"(zaa) comply with a requirement imposed by regulation 8ZA;";

(b) for sub-paragraph (b) substitute—

"(b) give a notification in relation to an incident as required by regulation 11(2);";

(c) for sub-paragraph (c) substitute—

"(c) comply with regulation 11(6) and (7) in relation to a notification under regulation 11(2);

(ca) comply with regulation 11(8);

(cb) give a notification in relation to an incident as required by regulation 11A(2);

(cc) comply with regulation 11A(6) and (7) in relation to a notification under regulation 11A(2);

(cd) comply with regulation 11A(8);

(ce) comply with a direction given to it under regulation 11B(6)(b);

(cf) comply with regulation 11B(12), 12B(11) or 14F(11) in relation to the making of a further disclosure as mentioned in the provision in question;

(cg) comply with regulation 11C(2)(b) and (4);

(ch) comply with regulation 11C(5); or";

(d) omit sub-paragraph (d);

(e) omit sub-paragraph (e) (including the "or" at the end).

(3) In paragraph (2)—

(a) in sub-paragraph (a), omit "or (2)";

(b) for sub-paragraph (b) substitute—

"(b) give a notification in relation to an incident as required by regulation 12A(1);";

(c) for sub-paragraph (c) substitute—

"(c) comply with regulation 12A(5) and (6) in relation to a notification under regulation 12A(1);

(ca) comply with regulation 12A(7);";

(d) in sub-paragraph (d) for "12(12)" substitute "12B(4)(b)";

(e) after sub-paragraph (d) insert—

"(dza) comply with regulation 11B(12), 12B(11) or 14F(11) in relation to the making of a further disclosure as mentioned in the provision in question;

(dzb) comply with regulation 12C(1)(b) and (3);

(dzc) comply with regulation 12C(4);

(dzd) comply with regulation 14(2) or (3);";

(f) in sub-paragraph (da), after "14A;" insert "or";

(g) omit sub-paragraph (e) (including the "or" at the end).

(4) After paragraph (2) insert—

"(2ZA) Subject to paragraph (2A), the Information Commission may serve an enforcement notice upon an RMSP if the Information Commission has

reasonable grounds to believe that the RMSP has failed to comply with any of the following—

(a) the duty imposed on it by regulation 14B(1);

(b) the requirements imposed by regulation 14C(2) or (5);

(c) the requirements imposed by regulation 14D;

(d) the duty to give a notification in relation to an incident as required by regulation 14E(1);

(e) the requirements in regulation 14E(5) and (6) in relation to a notification under regulation 14E(1);

(f) the duty in regulation 14E(7);

(g) a direction given to it under regulation 14F(4)(b);

(h) regulation 11B(12), 12B(11) or 14F(11) in relation to the making of a further disclosure as mentioned in the provision in question;

(i) the duty in regulation 14G(1)(b) and (3);

(j) the duty in regulation 14G(4);

(k) a direction given to it under regulation 16(2)(c);

(l) the requirements set out in regulation 16(3).

(2ZB) Subject to paragraph (2A), a designated competent authority or the Information Commission may serve an enforcement notice on a person if the authority or the Information Commission (as the case may be) has reasonable grounds to believe that the person has failed to comply with an information notice given by it to the person under regulation 15."

(5) In paragraph (2A)—

(a) for "paragraph (1) or (2)" substitute "this regulation";

(b) for "the OES or RDSP" substitute "the person on which the notice is to be served".

(6) In paragraph (2B)—

(a) for "the OES or RDSP" substitute "a person";

(b) after "provide" insert "the person with".

(7) In paragraph (2C)—

(a) for "the OES or RDSP", in the first place it occurs, substitute "the person in question";

(b) for "the OES or RDSP", in the second place it occurs, substitute "that person".

(8) In paragraph (3), for "paragraph (1) or (2)" substitute "this regulation".

(9) After paragraph (3) insert—

"(3ZA) The steps which may be specified under paragraph (3)(c) include steps outside the United Kingdom."

(10) For paragraph (3A) substitute—

"(3A) A person on which an enforcement notice has been served under this regulation must comply with the requirements, if any, of the notice regardless of whether the person has paid any penalty imposed on them under regulation 18."

(11) In paragraph (4), for "the OES or the RDSP, as the case may be," substitute "the person in question".

(12) In paragraph (5), for "The OES or RDSP" substitute "The person in question".

4 (1) Regulation 19A (appeal to the First-tier Tribunal) is amended as follows.

(2) In paragraph (1)(c), after "17(1)" insert "or (2ZB)".

(3) In paragraph (1)(d), for "18(3A)" substitute "18(3B)".

(4) In paragraph (2)(a), after "17(2)" insert "or (2ZB)".

(5) After paragraph (2) insert—

"(2A) An RMSP may appeal to the First-tier Tribunal against one or both of the following decisions of the Information Commission on one or more of the grounds specified in paragraph (3)—

(a) a decision under regulation 17(2ZA) or (2ZB) to serve an enforcement notice on that RMSP;

(b) a decision under regulation 18(3B) to serve a penalty notice on that RMSP.

(2B) A person may appeal to the First-tier Tribunal against any of the following decisions of a designated competent authority or of the Information Commission, on one or more of the grounds specified in paragraph (3)—

(a) a decision under regulation 14H to designate that person;

(b) a decision under regulation 14K to revoke that person's designation under regulation 14H;

(c) a decision under regulation 17(2ZB) to serve an enforcement notice on that person;

(d) a decision under regulation 18(3B) to serve a penalty notice on that person."

(6) In paragraph (3)—

(a) in the words before sub-paragraph (a), for "and (2)" substitute ", (2), (2A) and (2B)";

(b) in each of sub-paragraphs (b) and (d), for "or RDSP" substitute ", RDSP, RMSP or other person".

(7) In the heading, omit "by an OES or RDSP".

5 (1) In regulation 19B (decision of the First-tier Tribunal), paragraph (2) is amended as follows.

(2) After sub-paragraph (b) insert—

"(ba) a decision to designate a person under regulation 14H;

(bb) a decision under regulation 14K to revoke a person's designation under regulation 14H;".

(3) For sub-paragraphs (c) and (d) substitute—

"(c) a decision under regulation 17 to serve an enforcement notice; or".

(4) Omit sub-paragraph (e) (including the "or" at the end).

6 (1) Regulation A20 (enforcement by civil proceedings) is amended as follows.

(2) For paragraph (1) substitute—

"(1) This regulation applies where a designated competent authority or the Information Commission has reasonable grounds to believe that a person served with an enforcement notice under regulation 17 by them has failed to comply with the requirements of that notice as required by paragraph (3A) of that regulation."

(3) In paragraph (2), for "OES or RDSP" substitute "person on which the enforcement notice was served".

(4) In paragraph (3), for "an OES or RDSP" substitute "the person".

(5) In paragraph (4), for the words before paragraph (a) substitute "The designated competent authority or the Information Commission which served the enforcement notice may commence civil proceedings against the person in question—".

(6) Omit paragraph (5).

(7) In paragraph (6), for "OES or, as the case may be, RDSP" substitute "person in question".

7 (1) Regulation 23 (enforcement action - general considerations) is amended as follows.

(2) In paragraph (1)—

(a) for "or (2)" substitute ", (2), (2ZA) or (2ZB)";

(b) for "18(3A) or (3B)" substitute "18(3B)".

(3) In paragraph (2)—

(a) in paragraph (a), for "OES or RDSP, as the case may be," substitute "person in receipt of the enforcement notice or penalty notice, or against which civil proceedings have been commenced,";

(b) in each of paragraphs (b), (c) and (d), for "the OES or RDSP" substitute "the person".

SCHEDULE 2

Section 23

MINOR AND CONSEQUENTIAL AMENDMENTS ETC

The NIS Regulations

1 The NIS Regulations are amended as follows.

2 In regulation 1 (interpretation)—

(a) in paragraph (2)—

(i) omit the definition of "EU Regulation 2018/151";

(ii) after the definition of "critical supplier" (inserted by section 12(2)) insert—

""CSIRT" means the person designated by regulation 5 (computer security incident response team);";

(iii) omit the "and" at the end of the definition of "relevant law-enforcement authority";

(iv) in the definition of "representative", after "RDSP" (substituted by section 7(6)) insert "or an RMSP";

(v) omit the "and" at the end of the definition of "representative";

(vi) after the definition of "risk" insert—

""SPOC" means the person designated by regulation 4 (single point of contact).";

(b) in paragraph (3), omit sub-paragraph (c).

3 Omit regulation 2 (the NIS national strategy).

4 Omit regulation 3(6) (requirement for competent authorities to have regard to NIS national strategy).

5 In regulation 4 (designation of the single point of contact), in paragraph (3)(a), for "regulation 11(9) and 12(15)" substitute "regulations 11B(13), 12B(12) and 14F(12)".

6 (1) Regulation 5 (designation of computer security incident response team) is amended as follows.

(2) In paragraph (1)—

(a) after "sectors and" insert "relevant";

(b) after "services" insert "and managed services".

(3) For paragraph (2)(c) substitute—

"(c) consider whether and how to exercise its functions in response to any incident in relation to which it has been provided with a copy of a notification by virtue of regulation 11(8), 11A(8), 12A(7) or 14E(7);".

7 In regulation 8A (nomination by OES of person to act on its behalf in United Kingdom)—

(a) in paragraph (1), for "head office" substitute "principal office";

(b) in paragraph (4), for the words from "paragraph" to the end substitute "paragraph (3) 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 person nominated, the day on which the change took effect;

(b) where the change is to the nominated person's name, address or contact details, the day on which the OES became aware of the change.";

(c) in paragraph (5), for "responsibilities" substitute "functions".

8 In regulation 10(2) (security duties of operators of essential services), omit ", with a view to ensuring the continuity of those services".

9 In Part 4, for the Part heading substitute "Relevant digital service providers".

10 In regulation 13 (power of Information Commission to co-operate with the European Union), for "digital service providers" substitute "providers of relevant digital services".

11 In regulation 18(2) (penalties), for "regulation (3A)" substitute "regulation 17(3A)".

12 Omit regulation 21.

13 (1) Regulation 24 (service of documents) is amended as follows.

(2) In paragraph (1)—

(a) in the words before sub-paragraph (a)—

(i) for "or notice" substitute ", notice or direction";

(ii) after "served on" insert "or given to";

(iii) after "served", in the second place it occurs, insert "or given";

(b) omit the "or" at the end of sub-paragraph (b);

(c) for sub-paragraph (c) substitute—

"(c) sending it by post to the person's proper address or by email to the person's email address."

(3) In each of paragraphs (2) and (3)—

(a) after "document" insert ", notice or direction";

(b) after "served on" insert "or given to".

(4) In paragraph (4), for "service" substitute "documents, notices and directions".

(5) For paragraph (5) substitute—

"(5) For the purposes of this regulation, a person's "proper address" is—

(a) in a case where the person is a body corporate with a registered office in the United Kingdom, that office;

(b) in a case where paragraph (a) does not apply and the person is a body corporate, partnership or unincorporated body with a principal office in the United Kingdom, that office;

(c) in any other case, an address in the United Kingdom at which the person serving or giving the document, notice or direction believes, on reasonable grounds, that it will come to the attention of the person on whom it is to be served or to whom it is to be given.

(6) For the purposes of this regulation, a person's email address is—

(a) an email address provided to a NIS enforcement authority as an address for contacting that person,

(b) an email address published for the time being by that person as an address for contacting that person, or

(c) if no email address has been so provided or published, an email address by means of which the person serving or giving the document, notice or direction believes, on reasonable grounds, that it will come to the attention of that person."

(6) After paragraph (5A) (inserted by sub-paragraph (5)) insert—

"(5B) A document, notice or direction sent to a person by email is, unless the contrary is proved, to be treated as having been served or given at 9am on the working day immediately following the day on which it was sent.

(5C) In paragraph (5B) "working day" means a day other than a Saturday, a Sunday, Christmas Day, Good Friday or a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom."

14 Omit regulation 25.

15 Regulations 2 and 3(6) of the NIS Regulations continue to have effect, despite their revocation by paragraphs 3 and 4, until the first statement is designated for the purposes of section 25.

Other enactments

16 In Schedule 15 to the Enterprise Act 2002 (enactments conferring functions for the purposes of which public authorities may disclose information), in the entry relating to the Network and Information Systems Regulations 2018, for "Part 4" substitute "Parts 4 and 4A".

17 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 is revoked.

Cyber Security and Resilience (Network and Information Systems) Bill

[AS AMENDED ON REPORT]

A

B I L L

TO

Make provision, including provision amending the Network and Information Systems Regulations 2018, about the security and resilience of network and information systems used or relied on in connection with the carrying on of essential activities.

Brought from the Commons on 17th June 2026

Ordered to be Printed, 26th October 2026.

© Parliamentary copyright House of Commons and House of Lords 2026
This publication may be reproduced under the terms of the Open Parliament Licence, which is published at www.parliament.uk/site-information/copyright

PUBLISHED BY THE AUTHORITY OF THE HOUSE OF LORDS