STATUTORY INSTRUMENTS

2018 No. 506

The Network and Information Systems Regulations 2018

PART 2

The National Framework

The NIS national strategy

2.—(1) A Minister of the Crown must designate and publish a strategy to provide strategic objectives and priorities on the security of network and information systems in the United Kingdom ("the NIS national strategy").

(2) The strategic objectives and priorities set out in the NIS national strategy must be aimed at achieving and maintaining a high level of security of network and information systems in—

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

(b) digital services.

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

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

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

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

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

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

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

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

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

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

(6) The Minister must communicate the NIS national strategy, including any revised NIS national strategy, to the Commission within three months after the date on which the strategy is designated under paragraph (1).

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

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

(**1**) 1975 c. 26.

Designation of national competent authorities

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

(2) The Information Commissioner is designated as the competent authority for the United Kingdom for RDSPs.

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

(a) review the application of these Regulations;

(b) prepare and publish guidance;

(c) keep a list of all the operators of essential services who are designated, or deemed to be designated, under regulation 8, including an indication of the importance of each operator in relation to the subsector in relation to which it provides an essential service;

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

(e) send a copy of the lists mentioned in sub-paragraphs (c) and (d) to GCHQ, as the SPOC designated under regulation 4, to enable it to prepare the report mentioned in regulation 4(3);

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

(g) in order to fulfil the requirements of these Regulations, consult and co-operate with—

(i) relevant law-enforcement authorities;

(ii) competent authorities in other Member States;

(iii) other competent authorities in the United Kingdom;

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

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

(4) In relation to digital services, the Information Commissioner must—

(a) review the application of these Regulations;

(b) prepare and publish guidance; and

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

(5) The guidance that is published by under paragraph (3)(b) or (4)(b) may be—

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

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

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

Designation of the single point of contact

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

(2) The SPOC must—

(a) liaise with the relevant authorities in other Member States, the Cooperation Group and the CSIRTs network to ensure cross-border co-operation;

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

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

(3) The SPOC must submit reports to—

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

(b) the Commission identifying the number of operators of essential services for each subsector listed in Schedule 2, indicating their importance in relation to that sector.

(4) The first report mentioned in paragraph (3)(a) must be submitted on or before 9th August 2018 and subsequent reports must be submitted at annual intervals.

(5) The first report mentioned in paragraph (3)(b) must be submitted on or before 9th November 2018 and subsequent reports must be submitted at biennial intervals.

Designation of computer security incident response team

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

(2) The CSIRT must—

(a) monitor incidents in the United Kingdom;

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

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

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

(e) participate and co-operate in the CSIRTs network;

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

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

(i) incident and risk handling procedures, and

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

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

(3) The CSIRT may participate in international co-operation networks if the CSIRT considers it appropriate to do so.

Information sharing – enforcement authorities

6.—(1) The NIS enforcement authorities may share information with the CSIRT, the Commission and the relevant authorities in other Member States if that information sharing is—

(a) necessary for the requirements of these Regulations, and

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

(2) When sharing information with the Commission or the relevant authorities in other Member States under paragraph (1), the NIS enforcement authorities are not required to share—

(a) confidential information, or

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

Information sharing – Northern Ireland

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

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

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

(2) In this regulation—

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

(b) "a Northern Ireland Department" means a department mentioned in Schedule 1 to the Departments Act (Northern Ireland) 2016(**2**).

(**2**) 2016 c. 5.