Cyber Security and Resilience (Network and Information Systems) Bill

Explanatory Notes

What these notes do

These Explanatory Notes relate to the Cyber Security and Resilience (Network and Information Systems) Bill as introduced in the House of Commons on 12 November 2025 [HC Bill 329].

- These Explanatory Notes have been provided by the Department for Science, Innovation and Technology and the Department for Energy Security and Net Zero in order to assist the reader of the Cyber Security and Resilience (Network and Information Systems) Bill. They do not form part of the Cyber Security and Resilience (Network and Information Systems) Bill and have not been endorsed by Parliament.

- These Explanatory Notes explain what each part of the Cyber Security and Resilience (Network and Information Systems) Bill will mean in practice; provide background information on the development of policy; and provide additional information on how the Cyber Security and Resilience (Network and Information Systems) Bill will affect existing legislation in this area.

- These Explanatory Notes may best be read alongside the Cyber Security and Resilience (Network and Information Systems) Bill. They are not, and are not intended to be, a comprehensive description of the Bill.

Contents

Overview of the Bill

1. The Cyber Security and Resilience (Network and Information Systems) Bill (the "Bill") makes updates to the UK's only cross-sector cyber regulations, the Network and Information Systems Regulations 2018 (S.I. 2018/506) (NIS Regulations), as well as delivering new powers to ensure government can respond to new and emerging cyber threats.

2. The Bill will update the NIS Regulations by bringing more entities into their scope and equipping regulators with proportionate powers to better fulfil their duties. The Bill will provide the government with powers to amend and add to the NIS Regulations in the future and respond to imminent and actual threats to United Kingdom (UK) national security. These reforms are intended to better protect the services and other activities that are essential to the day-to-day functioning of society in the UK, and the economy, through safeguarding relevant network and information systems (the systems that allow computers and other devices to communicate with each other) and their surrounding environment.

Structure of the Bill

3. Part 2 of the Bill makes amendments to the NIS Regulations to bring new services (data centres, load control and managed services) into their scope, enable regulators to designate "critical suppliers", update the incident reporting regime, and make changes relating to recovery of costs, the sharing and gathering of information and enforcement.

4. Part 3 of the Bill provides the Secretary of State with powers to make regulations to update the regulatory framework. These include bringing more sectors into the scope of the NIS Regulations, setting duties and security requirements regulated persons must comply with, and issuing a code of practice to aid compliance with those regulations. Part 3 also enables the Secretary of State to designate a statement of strategic priorities that regulators will have a duty to have regard to. Finally, Part 3 requires the Secretary of State to report on cyber security legislation.

5. Part 4 of the Bill provides the Secretary of State with powers to issue directions to regulators and regulated entities, where it is necessary and proportionate for national security.

Policy background

6. The NIS Regulations were transposed from European Union (EU) law in 2018, using the European Communities Act 1972. The UK Government does not have the appropriate powers to update the NIS Regulations following the UK's departure from the EU.

7. The NIS Regulations place cyber security requirements on operators of essential services (OESs) in the drinking water, health, energy, transport and digital infrastructure sectors, as well as relevant digital service providers (RDSPs). These include online marketplaces, online search engines and cloud computing services.

8. There are currently 12 regulators that oversee the NIS Regulations in their respective sectors. Organisations in scope of the NIS Regulations must take appropriate and proportionate security measures to manage the risks posed to the security of network and information systems on which they rely to provide their services, report incidents that significantly disrupt their services, and work with their regulator.

9. Recent evidence demonstrates that the threat picture is evolving and the technologies relied upon by essential services are changing, whilst recent reviews of the NIS Regulations indicate that those regulations are failing to keep pace (see paragraphs 10 and 11).

10. In the year preceding September 2025, the National Cyber Security Centre (NCSC), part of Government Communications Headquarters (GCHQ), managed 429 cyber incidents, 204 of which were nationally significant – meaning they had a substantial impact on national security, economic stability, or public safety. This is a sharp increase from the 89 nationally significant incidents the previous year.[1] Of these incidents, 18 were classified as "highly significant" in nature, marking a 50% increase from the previous year.[2] Across the economy, organisations in the UK are facing daily cyber attacks, with over 600,000 businesses suffering an attack last year.[3]

11. Recent attacks have also demonstrated the impact of the existing regulations on the UK's national security. In 2024, a managed service provider (MSP) providing payroll services to the Ministry of Defence was attacked, exposing the records of over 270,000 military personnel, reservists and veterans.[4] Separately, there is growing evidence of state-backed foreign actors using cyber techniques to target the UK and other countries. For example, NCSC assess that Iran-based threat actors remain aggressive in cyberspace and Iran is likely developing its cyber capabilities and willing to target the UK to fulfil its disruptive and destructive objectives. Further, in September 2024, the UK and international allies exposed a unit of Russia's military intelligence service for a campaign of malicious cyber activity targeting government and critical infrastructure organisations around the world[5]. Finally, Volt Typhoon is a cyber threat group attributed to the People's Republic of China, and has targeted energy, transport and water sectors in the United States (US).[6] These examples demonstrate the importance of ensuring the UK's cyber security legislative framework is robust against cyber actors who threaten national security.

12. The Post-Implementation Review (PIR) of the NIS Regulations – conducted in 2020 – found that although organisations were taking measures to ensure the security of their network and information systems, the rate of improvement needed to be accelerated.

---

[1] It's time to act - NCSC Annual Review 2025

[2] National Cyber Security Centre Annual Review 2024, p.21

[3] NCSC.gov.uk – Cyber Security Breaches Survey 2025

[4] Hansard – Defence Personnel Data Breach – 8 May 2024

[5] NCSC.gov.uk – UK and allies uncover Russian military unit carrying out cyber attacks and digital sabotage for the first time

[6] NCSC.gov.uk - NCSC and partners issue warning about state-sponsored cyber attackers hiding on critical infrastructure networks

It highlighted the reliance on the services in scope of the NIS Regulations and impact that the failure or compromise of them could have.[7]

13. The Second PIR– conducted in 2022 – concluded that the NIS Regulations are not working as intended in several key areas, such as the scope of the regulations and the small number of incident reports being submitted. [8] For instance, in 2019, 2020 and 2021, there were only 13, 12 and 22 NIS incidents reported, respectively. Regulators have highlighted the lack of reports as an issue, especially as several high-profile incidents have been reported in the press without crucial details about them being reported to the regulators, as required under the NIS Regulations. This limits regulators' ability to use important intelligence to plan effectively, issue guidance and support entities to bolster their cyber resilience.

14. Following the Second PIR review, the previous government held a public consultation on proposals to improve the UK's cyber resilience in January 2022. The proposals included seven measures to address the evolving cyber security threats faced by the UK, which form the basis of the measures in the Bill.[9]

15. Additionally, in 2022, the previous government consulted on requiring all organisations remotely controlling large amounts of electrical load (300MW in aggregate or more) to be brought into scope of NIS.[10] A second consultation in April 2024 built on these proposals and set out principles for developing the large load controller's cyber security assurance framework.[11] In 2024, the previous government also consulted on bringing data centres into scope of the NIS Regulations.

16. In the July 2024 King's Speech, the government announced it would introduce a Cyber Security and Resilience Bill to strengthen the UK's cyber defences and build the resilience of the UK's essential and digital services. On 1 April 2025, the government published a Cyber Security and Resilience Policy Statement, which built on the measures outlined in King's Speech to set out the scope and ambition of the Bill.[12] The policy statement introduced four new measures that it would consider for an appropriate legislative vehicle. These were: bringing data centres and large load controllers into scope of the NIS Regulations, a statement of strategic priorities and two new powers to enable the government to respond to national security threats. The Bill has been determined as the most appropriate legislative vehicle to deliver these measures and, as such, they have been included.

17. Since publication of the policy statement, the government has continued to refine the measures. Based on feedback from stakeholders, including from regulators, as well as evidence from the second PIR, an additional measure which amends the enforcement provisions in the NIS Regulations has been included in the Bill.

---

[7] Post-Implementation Review of the Network and Information Systems Regulations 2018, p.5

[8] Second Post-Implementation Review of the Network and Information Systems Regulations 2018

[9] Proposal for legislation to improve the UK's cyber resilience - GOV.UK

[10] Delivering a smart and secure electricity system: the interoperability and cyber security of energy smart appliances and remote load control - GOV.UK

[11] Delivering a smart and secure electricity system: implementation - GOV.UK

[12] Cyber security and resilience policy statement - GOV.UK

Legal background

18. The NIS Regulations were made under Section 2(2) of the European Communities Act 1972.[13] The NIS Directive aimed to encourage a culture of cyber security in the service sectors considered most vital for the UK's economy and society. The NIS Directive was supplemented by EU Regulation 2018/151,[14] which provided further detail on the security requirements in the NIS Directive, and applied directly to the UK by virtue of Section 2(1) of the European Communities Act 1972.

19. The NIS Regulations were subsequently amended by further regulations made under Section 2(2) of the European Communities Act 1972, as well as Section 8 of the European Union (Withdrawal) Act 2018. Following the UK's exit from the EU, the NIS Regulations and EU Regulation 2018/151 are assimilated law. There are no appropriate powers currently available to update these regulations in order to keep pace with changes in the services considered to be essential to the UK's economy and society, the technological landscape or the nature of threats to network and information systems.

20. This Bill will directly amend the NIS Regulations and revoke EU Regulation 2018/151.

21. It will also provide the Secretary of State with powers to:

    a. make regulations in order to update the framework in the future;

    b. issue a code of practice to aid compliance with such regulations;

    c. direct regulated entities or regulators; and

    d. designate a statement of strategic priorities.

Measures in the Bill

22. The main provisions in the Bill are:

23. **Bringing the following into the scope of the NIS Regulations:**

    a. **Managed service providers (MSPs)** – the Bill will bring some medium and large MSPs – referred to as Relevant Managed Service Providers (RMSPs) in the Bill – into scope of the NIS Regulations. MSPs are organisations who provide ongoing managed services to another organisation, via a connection to their network and information systems. For example, organisations who provide ongoing IT and

[13] These Regulations implemented Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive).

[14] Commission Implementing Regulation 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. (EU Regulation 2018/151).

cyber security services. MSPs may provide a range of services, including IT outsourcing, remote IT support, management of applications (such as email services, web hosting), IT infrastructure management and support, and managed security services (such as firewall management, threat detection and incident response). These services are delivered on an ongoing basis, with the MSP often responsible for maintaining, monitoring, and supporting the client's IT environment. Those RMSPs in scope will be subject to the same duties to those placed on RDSPs already within scope of the NIS Regulations. The Information Commission (formerly the Information Commissioner's Office, or ICO) will act as the regulator. This measure aims to improve the resilience of RMSPs operating in the UK, and by extension the risk to other organisations who rely on them.

b. **Data centre infrastructure** – UK data centre services at or above 1MW capacity will be brought into scope. Data centre services provided on an enterprise basis (which serve its own undertaking only) will be brought in scope if they are at or above 10MW capacity. These thresholds are intended to align with EU precedent and balance proportionality and protection. Data centre operators will be designated as OESs and will be subject to similar duties, although some difference may apply (e.g. in relation to incident reporting) compared to other OESs. Ofcom and the Department for Science, Innovation and Technology will act as the joint regulator. Data centres house and support the technology and data that underpins the public's digital lives, and their disruption or compromise could impact the public, businesses and national security. Despite this critical function, they are currently not subject to any minimum cyber security or resilience requirements. This measure aims to improve the resilience of data centre infrastructure.

c. **Large load controllers** – organisations that control 300MW of electrical load or more to remotely control consumer appliances will be designated as OESs under the NIS Regulations. The Department for Energy Security and Net Zero and Ofgem will act as the joint regulator. This measure aims to ensure large load controllers have proportionate safeguards in place, in line with other energy infrastructure.

24. **Enabling critical suppliers to be designated and regulated –** regulators will be granted powers to designate and regulate organisations as "critical suppliers". Regulators will be able to designate a supplier of goods or services to OES, RDSPs or RMSPs as critical, if the following criteria apply:

    a. the supplier relies on network and information systems for the purposes of that supply;

    b. an incident affecting those network and information systems could cause disruption to essential, digital or managed services they supply (or essential, digital or managed services generally); and

    c. that disruption is likely to have a significant impact on the economy or day-to-day functioning of society in all or part of the UK.

    This could happen, for example, because the incident disrupts the supplier from delivering their goods or services, or because the supplier's systems are used as a

route for attackers to target the essential or digital service provider. Requirements critical suppliers will need to meet, including with respect to network and information system security duties, and incident reporting, will be set through regulations.

25. **Strengthening incident reporting requirements** – by expanding the scope of what should be reported and updating the processes and timeframes for how information is shared with relevant organisations. This includes:

    a. Introducing a two-stage reporting structure that will require regulated entities to notify their regulator of a significant incident no later than 24 hours after becoming aware of that incident, followed by a full report within 72 hours. In addition, in parallel to reporting to their regulator, regulated entities will be required to send a copy of the incident notifications and full report to NCSC, in its capacity as the computer security incident response team (CSIRT). These reforms aim to ensure more timely information is provided to regulators and the NCSC, who can help organisations respond effectively to incidents, as well as assess whether others may be at risk. They also aim to enable regulators, the NCSC and government to build a national picture of cyber threats and attack trends, which can in turn help develop better defences and proactive alerts to protect the wider economy.

    b. Expanding the definition of a reportable incident to capture a broader range of incidents. Currently, an incident only has to be reported to a regulator if it is causing significant disruption to an essential and digital service. This does not capture attacks that have compromised the integrity or security of a system in a way which could have significant impacts in the future. Examples of this include pre-positioning (where attackers gain administrative access or presence within networks to enable future significant disruption) and ransomware incidents (where malicious software infects a victim's computer system, preventing or impairing access to IT systems, and facilitating the theft of personal or sensitive data – then demanding payment). Measures in the Bill will require regulated entities to report such incidents.

    c. Improving transparency by requiring RDSPs, RMSPs and data centre operators to alert customers who are likely to have been affected by a significant incident. This is intended to ensure customers can take appropriate action to mitigate or prevent the risk to their systems.

26. **Enabling the Secretary of State to designate a statement of strategic priorities to establish a unified set of expectations for the implementation of regulations.** The NIS Regulations apply across multiple sectors and are enforced by 12 regulators (13 after this Bill comes into force). Regulators will have a duty to seek to achieve objectives contained within the statement. Regulators will be consulted on a draft statement of strategic priorities before it is designated.

27. **Strengthening provisions to provide greater certainty on what information can be shared and with whom**. This aims to ensure that regulators under the NIS Regulations can share information with relevant public sector bodies (and vice versa).

28. **Updating existing duties for RDSPs and make equivalent provision for RMSPs and data centre operators to provide certain information to their relevant regulators at the point of registration or designation.** This will help the Information Commission (RDSPs and RMSPs) and Ofcom (Data centres) exercise their functions.

29. **A new cost recovery framework to expand the options regulators have for recovering costs.** Currently, regulators are not able to recover the costs for their full activities in line with the NIS Regulations and are constrained by a model of billing for past activity. The new cost recovery framework will allow regulators to recover the full costs associated with their NIS activities through a periodic fee. The use of this power will be underpinned by safeguards including transparency and consultation requirements.

30. **Creating a power for the Secretary of State to direct regulators or regulated entities to take action in response to cyber threats that put the UK's national security at risk.** These powers will carry proportionate safeguards.

31. **Providing the Secretary of State with powers to make regulations.** This includes the ability to bring more sectors into scope of the NIS Regulations and update and introduce security and resilience requirements for organisations within scope including in relation to supply chain risk management.

32. **Issuing a code of practice to help regulated entities comply with the NIS Regulations and any other regulations made under this Bill.**

Territorial extent and application

33. **Clause** 5**9** sets out that the Bill extends to England and Wales, Scotland and Northern Ireland.

34. The subject matter of the Bill is reserved but some clauses of the Bill will alter the executive functions of the regulators, some of whom are devolved governments. In line with the Sewel Convention, the Government will seek Legislative Consent Motions from the Scottish Parliament, Welsh Senedd and Northern Ireland Assembly on these clauses.

35. Further information can be found at **Annex A.**

Commentary on Provisions of the Bill

Part 1 - Introduction

Clause 1: Meaning of "the NIS Regulations"

36. **Clause 1** clarifies that references to "the NIS Regulations" in the Bill are to the Network and Information Systems Regulations 2018 (SI 2018/506).

Clause 2: Overview of Act

37. **Clause 2** provides an overview of the Bill and its structure (as described in paragraphs 3-5 of these explanatory notes).

Part 2 – The NIS Regulations

Chapter 1 – Persons regulated under the NIS Regulations

Clause 3: Identification of operators of essential services

38. **Clause 3** amends Regulation 8 of the NIS Regulations to clarify that OESs can be in scope of the NIS Regulations whether or not they are established in the UK, as long as they are operating an essential service in the UK.

39. Subsection (3) clarifies that a person cannot be an OES if they provide a public electronic telecommunications network (PECN) or a public electronic telecommunications service (PECS), as defined by section 151(1) of the Communications Act 2003.

Clause 4: Data centres to be regulated as essential services

40. **Clause 4** introduces Data infrastructure as a sector and subsector (by addition to the table in schedule 1 to the NIS Regulations). It also designates the Secretary of State for Science, Innovation and Technology and Ofcom as joint regulators. The clause also introduces a new paragraph 11 to Schedule 2 to the NIS Regulations to incorporate 'data centre services' as essential services in the data infrastructure sector. This formally integrates the 'data infrastructure' subsector into the framework for OESs. This clause captures entities managing a significant amount of commercial or enterprise data centre service. This clause also describes the essential services and threshold requirements for the new data infrastructure subsector.

The data infrastructure subsector

41. Subsection (3) adds paragraph 11 to schedule 2 to the NIS Regulations and describes the threshold requirements which apply to specified kinds of essential services in the data infrastructure subsector.

    a. Paragraph 11(2) identifies the first essential service and stipulates that a data centre service (other than a data centre service provided on an enterprise basis) with a rated IT load (the maximum electrical power available for the operation of relevant IT equipment) equal to or greater than 1 megawatt is within scope of the NIS Regulations.

b. Paragraph 11(3) stipulates that the essential service of the provision of a data centre service on an enterprise basis with a rated IT load equal to or greater than 10 megawatts will fall within scope of the regulations.

c. Paragraph 11(4) defines a "data centre service".

d. Paragraph 11(5) defines “Relevant IT Equipment” as referring to equipment used for the purposes of providing information technology services.

e. Paragraph 11(6) defines “supporting infrastructure” for the relevant IT equipment.

f. Paragraph 11(7) stipulates that data centre services are provided on an enterprise basis if the data centre is owned or managed by a person in connection with the carrying on of an undertaking by the person, and the sole purpose of the data centre is to provide information technology services for that undertaking.

g. Paragraph 11(8) defines “environmental control” and provides definitions for “rated IT load” (RITL) and “structure”.

Clause 5: Operators of data centre services: Crown application etc

42. **Clause 5** introduces new paragraphs (7ZA) and (7ZB) to regulation 8 of the NIS Regulations.

    a. Paragraph (7ZA) extends the application of paragraphs (1) and (3) to data centre services provided, as defined in schedule 2, paragraph 11 in the NIS Regulations by or on behalf of the Crown.

    b. Paragraph (7ZB) outlines exceptions where this extension does not apply:

        i. If the service is provided by the Security Service, the Secret Intelligence Service, or GCHQ.

        ii. If the service is provided commercially on behalf of His Majesty’s government, and that service enables the handling of information classified as “secret” or “top secret” under UK Government security classification policy.

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

43. **Clause 6** introduces new **s**ubparagraphs (5A) to (5E) to paragraph 1 of schedule 2 to the NIS Regulations to incorporate ‘load control’ as an essential service in the energy subsector – formally integrating ‘load controllers’ into the framework for OES. This clause captures entities managing a significant amount of electricity through relevant energy smart appliances (ESAs). New subparagraphs (5A) to (5E) describe the essential service and threshold requirements.

44. Subsection (1) amends paragraph 1 of schedule 2 to the NIS Regulations as set out in subsections (2) and (3) identifying the essential service and threshold requirements for load control under the electricity subsector.

45. Subsection (2) inserts new sub-paragraphs which set out the threshold requirements and extent of the activities that may lead to an organisation being designated as an essential service:

    a. Subparagraph (5A) sets out the threshold requirement for the essential service of load control as the potential electrical control of all relevant ESAs managed by the load controller as equal to or greater than 300 megawatts.

    b. Subparagraph (5B) defines the meaning of a load controller's "potential electrical control", which is the maximum aggregate flow of electricity into and out of all relevant ESAs managed by the load controller.

    c. Subparagraph (5C) sets out that the ESAs within scope of the essential service are electric vehicles, electric vehicle charge points, electrical heating appliances, battery energy storage systems and virtual power plants. An ESA is "managed" by a person if they control the electricity flowing into and out of it by sending load control signals.

    d. Subparagraphs (5D) and (5E) describes the application of the NIS Regulations in relation to different operating models of providing load control. Load controllers managing ESAs through third parties will be subject to the regulations. Where a third party is capable of adjusting or processing the load control signals being sent to an ESA and has been authorised by the load controller then both the load controller and third party will be subject to the regulations.

46. Subsection (3) amends subparagraph 8 in paragraph 1 of schedule 2 to the NIS Regulations to include definitions relevant to the essential service of load control. This includes defining certain relevant ESAs described in subparagraph (5C) and the meaning of "load control" and "load control signal" as defined under Part 9 of the Energy Act 2023. It is the intention of the Department for Energy and Net Zero to define the remaining relevant ESAs in regulations after Royal Assent.

Clause 7: Digital services

47. **Clause 7**, subsections (1) and (2) amend regulations 1(2) of the NIS Regulations, altering the definition of "cloud computing service", omitting the existing definitions of "digital service" and "digital service provider", and inserting a new definition for "relevant digital service", in accordance with subsections (3) to (5).

48. Subsection (3) updates the definition of a "cloud computing service" in the NIS Regulations. This includes setting out that a cloud computing service is not a managed service, to avoid regulatory overlap of these services.

49. Subsection (4) removes the previous definitions of "digital service," and "digital service provider" to align with the updated definitions provided by the Bill.

50. Subsection (5) inserts a new definition for “relevant digital service”.

51. Subsection (6) amends the definition of "representative" in the NIS Regulations by replacing “a digital service provider” with the term “RDSP”, which is separately defined in new paragraph (3)(e) (see below).

52. Subsection (7) inserts new paragraph 2A with a definition of “broad remote access” and “scalable and elastic” to further clarify the definition of “cloud computing service”.

53. Subsection (8) substitutes a new paragraph 3(e) to define “relevant digital service provider" (“RDSP”).

54. Subsection (9) inserts new paragraph 3A setting out that a person does not provide a relevant digital service if they provide a public electronic telecommunications network (PECN) or a public electronic telecommunications service (PECS), as defined by section 151(1) of the Communications Act 2003.

55. The Communications Act 2003, as amended by the Telecommunications (Security) Act 2021 (the TSA), places security duties on providers of Public Electronic Communications networks and services (PECNs and PECSs) to secure their networks and services. If providers of PECNS and PECS also provide digital services that meet the definition in subsection (3A), they will be in scope of this provision for the digital services that they provide.

Clause 8: Duties of relevant digital service providers

56. **Clause 8** amends regulation 12(2) of the NIS Regulations relating to the security requirements of RDSPs.

57. Subsection (2)(a) and (b) amend regulation 12(2), requiring RDSPs to prevent and minimise the impact of incidents affecting the security of their network and information systems, rather than focussing on the continuity of their services, and removes requirements to take into account Article 2 of EU Regulation 2018/151. Subsection (3) requires RDSP to have regard to guidance issued by the Information Commission as they carry out these duties.

Clause 9: Managed service providers

58. **Clause 9** amends regulation 1 of the NIS Regulations to insert the definition of a relevant managed service provider and the definition of a ‘managed service’.

59. Subsection (3) inserts the definition of ‘managed service’ in the NIS Regulations.

60. Subsection (4) inserts the definitions of a "relevant managed service provider" (RMSP) into the NIS Regulations. New subparagraph (3)(ea) of regulation 1 defines a managed service provider as a person (including an organisation) who:

    a. provides managed services in the UK whether or not the person is based in the UK.

b. is not designated as a critical supplier under regulation 14H in relation to the provision of that service.

c. is not a micro or small enterprise as defined in Commission Recommendation 2003/361/EC (a person or enterprise must employ 50 persons or more and their annual turnover and/or annual balance sheet total must exceed EUR 10 million to be in scope of the regulations).

d. is not subject to public authority oversight or is subject to public authority oversight but derives more than half of its income from commercial activities.

61. Subsection (5) inserts a new paragraph 3B to regulation 1 of the NIS Regulations to define a "managed service". This is a service which is both:

a. provided by a person under a contract entered into with 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).

b. provided to the customer by means of P, or a person acting on P's behalf, connecting to or otherwise accessing network and information systems relied on by the customer in connection with a business or other activity carried on by the customer.

62. Relating to this definition, new paragraph (3C) sets out that for the purposes of (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.

63. Paragraph (3D) confirms that a person does not provide a managed service by virtue of providing a data centre service as defined by paragraph 11(4) of schedule 2, or a PECNs or a PECSs, as defined by section 151(1) of the Communications Act 2003. This means that there will be no regulatory overlap of these services.

64. The Communications Act 2003, as amended by the Telecommunications (Security) Act 2021, places security duties on providers of PECNs and PECSs to secure their networks and services. If providers of PECNS and PECS also provide managed services that meet the definition in paragraph S1(3)(ea) and 3B), they will be in scope of this provision for the managed services that they provide.

Example: Operational Technology

A company that remotely manages IT systems used to monitor operational technology (e.g. for incident monitoring) on behalf of their business customer would be in scope as a managed service provider.

A company providing operational technology with no additional IT management, such as a scanner in airports, sensors used in gas/electricity networks, or industrial controls systems such as Supervisory Control and Data Acquisition (SCADA), would not be in scope as a managed service provider.

Example: Telecommunications

A company providing public telecommunications services, such as an internet access or phone connectivity, would not be considered a relevant managed service provider. However, if the same company provides managed services, such as managing the client's IT network security, monitoring IT infrastructure, or administering IT systems, these activities would be considered managed services under **Clause 9**, and within scope of the Regulations.

Clause 10: Duties of managed service providers to manage risks

65. **Clause 10** inserts new Part 4A, regulation 14B, RMSPs: duties to manage risks to network and information systems into the NIS Regulations.

    a. Paragraph (1) of new regulation 14B sets out the security duties placed on RMSPs. An RMSP must identify and take appropriate and proportionate steps to manage the risks posed to the security of the network and information systems that it is reliant on to provide its managed service in the UK. A similar duty is placed on RDSPs under regulation 12 of the NIS Regulations.

    b. Paragraph (2) provides more detail on the security measures in paragraph (1). An RMSP must ensure a level of security of network and information systems appropriate to the risk posed, while having regard to the state of the art (i.e. the state of technological development). Further, RMSPs must prevent and minimise the impact of incidents affecting the security of network and information systems relied on for providing their managed services. Further detail on what appropriate and proportionate actions an RMSP would be expected to take under this security duty will be set out in regulations made under **clause 29(1).**

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

66. **Clause 11** inserts a new paragraph 3E to regulation 1 of the NIS Regulations to define "subject to public authority oversight" for the purposes of paragraph (3)(e) and (ea).

Clause 12: Critical suppliers

67. **Clause 12** amends the NIS Regulations to insert a new Part 4B, which provides a framework for the designation, regulation and oversight of "critical suppliers". These are suppliers of goods or services to OESs, RDSPs or RMSPs, where the supplier relies on network and information systems for the purposes of that supply and an incident affecting those network and information systems could cause disruption to the essential, digital or managed services supplied to the OES, RDSP or RMSP (or essential, digital or managed services generally), and that disruption is likely to have a significant impact on the economy or day-to-day functioning of society in all or part of the UK. New Part 4B comprises regulations 14H to 14L. The security, incident reporting and other regulatory duties applicable to designated critical suppliers will be set out in regulations made under c**lause 29(1)**.

68. Subsection (2) inserts a new definition into regulation 1(2) of the NIS Regulations. It defines a “critical supplier” as a person who is designated under the new regulation 14H.

69. Subsection (3) introduces a new Part 4B into the NIS Regulations, which contains the framework for the designation of critical suppliers. This includes the powers of designation, the conditions of designation, restrictions on designation, procedural safeguards, and coordination duties between regulators.

Designation of critical suppliers

70. New regulation 14H provides the power for a regulator to designate a person ("P") as a critical supplier.

    a. Paragraphs (1) and (2) set out the general power of designation, subject to the conditions in paragraphs (1) to (7) and the limitations in new regulation 14I.

    b. Paragraphs (1)(a) and (2)(a) outline that to be designated as a supplier, P must supply goods or services directly—either to an Operator of Essential Services (OES) in respect of which the competent authority acts as regulator, or to a Relevant Digital Service Provider (RDSP) or a Relevant Managed Service Provider (RMSP), in the case of designation by the Information Commission.

    c. Paragraphs (1)(b) and (2)(b) outline that P must rely on network and information systems for the purposes of that supply.

    d. Paragraphs (1)(c)(i) and (2)(c)(i) outline that, in order to designate, the relevant regulator must consider that an incident affecting the operation or security of the network and information systems relied upon by P could disrupt:

        i. in the case of a competent authority (paragraph (1)): the provision of essential services by the OES to whom P supplies, or such services more widely through other persons to whom P supplies; or

        ii. in the case of the Information Commission (paragraph (2)): the provision of relevant digital services or managed services by the RDSP or RMSP to whom P supplies, or such services more widely through other persons to whom P supplies. This includes scenarios where the incident directly affects the supplier’s ability to continue supplying the goods or services in question; or otherwise causes disruption through interconnectivity or vector risk, even if the supply of goods or services is uninterrupted.

    e. Paragraphs (1)(c)(ii) and (2)(c)(ii) require the regulator to consider whether a disruption, caused by an incident affecting the supplier’s network and information systems, would likely have a significant impact on the UK’s economy or the day-to-day functioning of society, either nationally or in part.

    f. Paragraphs (1)(d) and (2)(d) outline that to designate P, the designation must not be prevented by regulation 14I.

g. Paragraph (3) requires that when assessing whether an incident could cause disruption for the purposes of regulation 14H(1)(c)(i) or 14H(2)(c)(i), the regulator must, in particular, have regard to whether the goods or services supplied by the person could be obtained from alternative sources in the event of such an incident.

h. Paragraph (4) requires that when assessing whether an incident could cause significant disruption for the purposes of regulation 14H(1)(c)(ii) or 14H(2)(c)(ii), the regulator must, in particular, have regard to the likely nature, scale and duration of the potential disruption to the provision of the relevant service or services.

i. Paragraph (5) sets out that designation may be made by more than one regulator, or by one or more regulators and the Information Commission.

j. Paragraph (6) sets out further factors that a regulator must consider before designating a supplier. These include:

    i. whether the risks associated with the supplier's services could instead be adequately managed by duties already imposed on the OES, RDSP or RMSP under the regulations.

    ii. whether another regulatory body already exercises some form of regulatory oversight of the supplier, through the NIS Regulations or another regulatory framework; and if so, whether that regulation is sufficient to manage the relevant risks.

k. Paragraph (7) confirms that the supply of goods that are in scope of the power of designation include those provided from outside the UK, as well as within in it; and that the power of designation applies to persons not established in the UK, as well as those that are.

l. Paragraph (8) clarifies that the power to designate a person as a critical supplier applies whether the relevant goods or services are supplied from within the UK or from outside it.

Example: Laboratory service provider to health sector

A diagnostic laboratory provider handles pathology testing services for an OES. The provider uses its own network and digital systems to manage test data, results and report generation. A ransomware attack affecting this supplier could halt the processing and delivery of test results, leading to delayed diagnoses and a widespread cancellation of appointments. Given the scale of disruption this could cause to essential healthcare services, the laboratory provider may be designated as a critical supplier.

Restrictions on designation

71. New Regulation 14I sets out specific cases in which a person cannot be designated as a critical supplier. A person may not be designated in respect of a service if they

already provide that service as—

a. an OES;

b. an RDSP; or

c. an RMSP.

Example: Existing OES exemption

A regional electricity distributor is already designated as an OES under the NIS Regulations. It cannot also be designated as a critical supplier in relation to that service, even if it meets the criteria for designation.

Designation: consultation and procedure

72. New Regulation 14J sets out the consultation and procedural steps that must be followed before a designation is confirmed.

a. Paragraph (1)(a), in conjunction with paragraph (2), requires the regulator to consult with any other regulator that has a relevant connection with the supplier (as defined in paragraph (3)); and any other person the regulator considers appropriate (e.g. the government).

b. Paragraph (1)(b) requires the regulator to provide the supplier with written notice of the proposed designation. The notice must explain the reasons for the proposed designation and give the supplier a reasonable period in which to respond with written representations.

c. Paragraph (1)(c) obliges the regulator to have regard to any representations received before making a final designation decision.

d. Paragraph (2) clarifies who must be consulted under paragraph (1)(a) by defining "relevant connection" for the purposes of the consultation duty. It is for the regulator to consider whether such a connection exists, requiring judgement based on the regulator's understanding of the supplier's relationships and potential impact.

e. Paragraph (3) explains what constitutes a relevant connection. In the case of a regulator other than the Information Commission, this will be so if:

i. The regulator has already designated the supplier, or

ii. The supplier provides goods or services to an OES regulated by that regulator.

In the case of the Information Commission, this will be so if:

i. The Information Commission has already designated the supplier, or

ii. The supplier provides goods or services to a RDSP or RMSP.

f. Paragraphs (4) and (5) apply where the regulator decides to proceed with designation following consultation, receipt of any written representations within the period they have specified to the supplier, and having had regard to those representations. In that case, the regulator must:

   i. Provide the supplier with a confirmation notice stating the reasons for designation and the date it takes effect;

   ii. Share a copy of this notice with any other parties consulted under paragraph (1)(a).

g. Paragraph (6) allows the regulator to change the effective date of the designation after issuing the notice by giving notice of the updated date to all recipients of the original notice.

Revocation of designation

73. New Regulation 14K provides for the revocation of a designation when a supplier no longer meets the criteria in regulation 14H.

a. Paragraph (1) and (2) give the regulator the power to revoke a designation made under regulation 14H if it is satisfied that the person no longer meets the designation conditions set out in regulation 14H(1)(a)–(d) or 14H(2)(a)–(d).

b. Paragraph (3) requires a person designated under regulation 14H by a regulator to notify that authority, as soon as practicable, if they have reasonable grounds to believe that the authority would no longer be able to designate them if they weren't already designated. The notification must be in writing and supported by evidence. Where the person believes their designation would also be prevented by regulation 14I(b) or (c) (because they are an RDSP or RMSP), they must also notify the Information Commission.

c. Paragraph (4) requires the regulator to have regard to a notification and any supporting evidence given when considering whether to revoke the designation.

d. Paragraph (5) places a parallel duty on persons designated under regulation 14H by the Information Commission. If they have reasonable grounds to believe that the Information Commission would no longer be able to designate them, they must promptly notify the Information Commission in writing and provide supporting evidence.

e. Paragraph (6) requires the Information Commission, on receipt of such a notification and supporting evidence, to have regard to it when considering whether to revoke the designation.

f. Paragraph (7) applies the consultation and procedural provisions in regulation 14J to revocations under this Regulation. This includes the requirement to consult

relevant regulators and to give the supplier an opportunity to make representations before a final decision is made.

Example – Revocation of designation following change in operations:

A company that had been designated as a critical supplier to a national water utility (an OES) was initially relied upon to supply specialist hardware sensors integral to the real-time monitoring of the water system. However, the OES has since migrated to a different solution that no longer requires the services from the original supplier. As a result, the critical supplier submits evidence to the regulator showing that the service is no longer in use.

After consulting the OES, the regulator determines that the supplier could no longer have a 'disruptive effect' on water supply. It therefore issues a notice revoking the designation.

Co-ordination

74. New regulation 14L introduces a requirement for regulators to coordinate their activities when exercising functions under the regulations in relation to critical suppliers.

    a. Paragraph (1) requires a regulator that has designated a person ("P") as a critical supplier to coordinate with both:

        i. any other designated regulator that has also designated P, and

        ii. the Information Commission, if the Information Commission has designated P.

    b. Paragraph (2) mirrors this obligation for the Information Commission, requiring them to coordinate with any regulator that has also designated a person who the Information Commission has designated.

    c. Paragraph (3) introduces a separate coordination duty that applies when relevant regulators are considering whether to designate a person.

    d. Paragraph (4) defines when a regulator is considered "relevant" for the purposes of these coordination duties. This definition is central to the coordination duty outlined in paragraph (3) which requires regulators to work together when designating a supplier as critical. A regulator is considered relevant if:

        i. they have already designated the person in question, or

        ii. it is reasonable to assume that the person may meet the criteria for designation by that regulator.

    e. Paragraph (5) requires regulators to use their powers under regulation 15(1) to formally request relevant information from one another as part of their

coordination duties, where the other regulator may be expected to hold useful information.

f. Paragraph (6) provides that regulators are not required to comply with the coordination duties where doing so would impose a burden disproportionate to the benefit.

g. Paragraph (7) clarifies that these coordination duties do not replace or limit the general consultation and cooperation duties that already apply to regulators under regulation 3 of the NIS Regulations.

h. Paragraph (8) sets out what is meant by "meets the requirements for designation" in this regulation. A person meets the requirements if they satisfy the designation conditions in regulation 14H(1)(a)–(d) or 14H(2)(a)–(d), including that they not excluded by any of the restrictions in regulation 14I.

Example: Coordinated designation of a shared critical supplier

A company supplies services to OESs in both the water and energy sectors. Though the services differ, they are both supported by the same underlying network and information systems.

Regulators for each sector independently assess the services and conclude that they meet the threshold for designation as a critical supplier and the supplier does not fall within one of the exceptions under regulation 14I. After consulting each other under regulation 14J, both regulators proceed with designation.

Under the coordination duty in regulation 14L, the regulators agree to streamline the designation process. They share relevant information, align the timing of their designation notices, consultation periods and coordinate messaging to the supplier. Each regulator then issues its own designation notice, tailored to the service used in their sector.

Chapter 2: Provision of information and reporting of incidents

Clause 13: Provision of information by operators of data centres

75. **Clause 13** amends the NIS Regulations to set out the duties of data centre operators to provide information to their regulators. This ensures that data centre operators, which are entities providing vital services such as data storage and processing, are subject to specific information-sharing controls.

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

76. Subsection (2) inserts New Regulation 8ZA into the NIS Regulations. It requires data centre operators to provide information to the joint regulators (Ofcom and the Department for Science, Innovation and Technology) when they are designated under regulation 8.

a. Paragraph (1) outlines who the regulation applies to. It covers data centre operators who are either deemed designated under regulation 8(1), or

designated under regulation 8(3), as an OES in the data infrastructure subsector.

b. Paragraph (2) sets out information which must be provided to the regulator and the deadline by which data centre operators must provide the required information to the regulator for the purpose of enabling the regulator to maintain the list mentioned under regulation 8(8). This is within three months of either being deemed designated under regulation 8(1), or receiving a designation notice under regulation 8(5).

c. Paragraph (3) sets out the information data centre operators must provide to the regulator. Paragraph (4) defines the "relevant 3-month period" for submitting this information.

    i. For operators deemed designated under regulation 8(1), the period begins on the first day of designation.

    ii. For operators formally designated under regulation 8(5), the period begins on the day the designation notice is served.

d. Paragraph (5) clarifies the meaning of "proper address" depending on the operator's legal structure.

e. Paragraph (6) requires data centre operators to notify the regulator of any changes to the specified information within 7 days of the change.

f. Paragraph (7) defines the term "data centre service" for the purposes of this regulation as an essential service as described in paragraphs 11(2) or 11(3) of Schedule 2 to the NIS Regulations.

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

77. **Clause 14** amends the NIS Regulations to update the duty for RDSPs and RMSPs to provide information to the Information Commission at registration, sets out when they need to register this information, and the duties for RMSPs established outside the UK.

78. Subsection (2) amends regulation 14 of the NIS Regulations, which relates to registration with the Information Commission.

    a. Subsection 2(a) amends sub-paragraph of regulation 14 to set out that an RDSP must provide to the Information Commission, the RDSP's proper address, and information on the type of service it provides i.e. cloud computing service, online search engine, online marketplace. Subsection (2)(b) inserts new paragraph (2A) to clarify the meaning of "proper address" depending on the RDSP's legal structure.

b. Subsection (2)(c) requires RDSPs to notify the Information Commission of any changes to the specified information as soon as reasonably practicable, and in any event within 7 days of the change.

c. Subsection (2)(d) sets out the deadline for an RDSP to register. This is within three months of this clause coming into force, or in any other case, within the three months of the organisation subsequently satisfying the conditions for being an RDSP.

d. Subsection (2)(e) requires the Information Commission to send a copy of the register of RDSPs to GCHQ for the purpose of exercising its functions under or by virtue of these regulations or any other enactment, within four months of this **clause 14** coming into force and subsequently, at annual intervals.

79. Subsection (3) amends regulation 14A of the NIS Regulations for those RDSPs established outside the UK.

80. Subsection (4) substitutes a new Paragraph 1 in regulation 14A to specify that it applies to RDSPs which have their principal office outside the UK.

81. Subsection (5) substitutes “digital service provider” for “RDSP” and inserts a requirement to provide an email address and telephone number for any nominated representative.

82. Subsection (6) substitutes a new paragraph 3 and 3(A) to specify when the RDSP must comply with the requirements to nominate a representative in the UK, before the end of three months after this clause comes into force, or, in any other cases, within three months of the RDSP becoming an RDSP. Paragraph 3A requires RDSPs to notify the Information Commission of any changes to the specified information as soon as reasonably practicable, and in any event within 7 days of the change taking effect, for a change to the representative nominated, or within 7 days of the RDSP becoming aware of the change, for a change in the representative’s name and contact details. Subsection (6) also substitutes a new paragraph 4 to enable the Information Commission or GCHQ to contact the representative instead of, or in addition to the RDSP, for the purposes of carrying out their functions.

Registration of RMSPs with the Information Commission

83. Subsection (9) adds new regulation 14C to the NIS Regulations to set out the duties of RMSPs to provide information to the Information Commission.

a. Paragraph (1) requires the Information Commission to maintain a register of all RMSPs that have registered with it.

b. Paragraphs (2) to (5) set out further detail on the requirements relating to the registration of RMSPs with the Information Commission, these details are all consistent with the relevant sections relating to the registration of RDSPs with the Information Commission (except only RDSPs are required to set out which relevant digital services they provide).

c. Paragraph (6) requires the Information Commission to send a copy of the register of RMSPs to GCHQ for the purpose of exercising its functions under or by virtue of these regulations or any other enactment, within four months of this Clause coming into force and subsequently, at annual intervals.

Representatives of RMSPs established outside the United Kingdom

a. Subsection (9) adds new Regulation 14D to the NIS Regulations to set out the duties of RMSPs to register where they have its principal office outside the UK.

b. Paragraph (1) of regulation 14D introduces registration requirements for an RMSP which has its principal office outside the UK.

c. Paragraph (2) requires the RMSP to nominate a UK representative and notify the Information Commission of the UK representative's name and contact details in writing.

d. Paragraph (3) specifies that the RMSP must appoint and notify the Information Commission of its nominated UK representative before the end of three months of this clause coming into force or, in any other cases, within three months of the RMSP meeting the conditions for being an RMSP.

e. Paragraph (4) requires the RMSP to notify the Information Commission of any changes to the specified information as soon as reasonably practicable, and in any event within 7 days of the change taking effect, for a change to the representative nominated, or within 7 days of the RMSP becoming aware of the change, for a change in the representative's name and contact details.

f. Paragraph (5) sets out that the Information Commission or GCHQ may contact the nominated representative instead of, or in addition to the RMSP, for the purposes of carrying out their functions

g. Paragraph (6) states that a nomination under paragraph (2) is without prejudice to any legal action which could be initiated against the RMSP in question.

Clause 15: Reporting of incidents by regulated persons

84. **Clause 15** amends the requirements for reporting incidents in the NIS Regulations.

85. Subsection (2) amends the definition of 'incident' in the regulations, so that it includes events having, *or capable of having,* an actual adverse effect on the *operation or* security of network and information systems. The change to the definition is designed to include incidents that have compromised the integrity or security of a system without causing significant disruption yet, but that could have potential significant impacts in the future. Examples of this include pre-positioning (where attackers gain administrative access or presence within networks to enable future exploitation) and ransomware incidents.

86. Subsection (3) substitutes new regulation 11 of the NIS Regulations, to include measures around the notification of incidents affecting OESs other than in relation to data centre services.

Notification of incidents (other than in relation to data centre services)

a. Paragraph (1) of new regulation 11 sets out that the following regulation applies to OESs, with the exception of data centre services (for which new regulation 11A applies).

b. Paragraph (2)(a) details that, if an OES is aware than an OES incident has occurred or is occurring, it must send an initial notification to its regulator. The initial notification must include the OES's name, the essential service to which the incident relates, and brief details of the incident.

c. Paragraph (2)(b) adds that a full notification must also be sent to the OES's regulator. The full notification must include the information set out at paragraph (5), but only insofar as that information is known to the OES.

d. Paragraph (3) states that an OES incident is an incident that has affected the operation or security of the network and information systems relied on to provide the essential service, and the incident has had or is likely to have a significant impact in relation to the whole or part of the UK, having regard to the factors listed in paragraph (4).

e. Paragraph (4) lists factors to which an OES must have regard in determining whether an incident has had, is having, or is likely to have a significant impact.

f. Paragraph (5) lists the information that must be included in a full notification, insofar as the information is known to the OES.

g. Paragraph (6) sets out the timescales in which the notifications must be sent. The initial notification, containing brief details of the incident, must be sent within 24 hours of the OES becoming aware of the OES incident. The full notification must be sent within 72 hours of the OES being aware of the OES incident.

h. Paragraph (7) states that a notification, whether it be an initial notification or a full notification, must be in writing, and must take the form and manner as determined by the relevant regulator.

i. Paragraph (8) states that an OES must send a copy of a notification to the CSIRT at the same time as sending the notification to its regulator.

j. Paragraph (9) specifies that in new regulation 11, 11A and 11B, "regulated person" means an OES, an RDSP, an RMSP or a critical supplier.

Notification incidents in relation to data centres services

87. Subsection (3) also adds new regulation 11A to the NIS Regulations, relating to the notification of incidents in relation to data centre services.

a. Paragraph (1) of new regulation 11A states that the following requirements apply to an OES that provides a data centre service.

b. Paragraph 2(a) details that, if an operator of a data centre is aware than a data centre incident has occurred or is occurring, it must send an initial notification to

its regulator. The initial notification must include the operator of the data centre's name; the data centre service to which the incident relates; and brief details of the incident.

c. Paragraph 2(b) adds that a full notification must also be sent to the relevant regulator. The full notification must include the information set out at paragraph (4), but only insofar as that information is known to the operator of the data centre service.

d. Paragraph (3) states that a data centre incident is an incident that has had, could have had, is having, or is likely to have a significant impact on the continuity of the data centre service provided by the operator, on the operation or security of the network and information systems on which the operator of the data centre relies in order to provide the data centre service, or any other impact in all or any part of the UK which is significant.

e. Paragraph (4) lists the information that must be included in a full notification, insofar as the information is known to the operator of the data centre service.

f. Paragraph (5) sets out the timescales in which the notifications must be sent. The initial notification, containing brief details of the incident, must be sent within 24 hours of the operator of the data centre service becoming aware of the data centre incident. The full notification must be sent within 72 hours of the operator of the data centre being aware of the incident.

g. Paragraph (6) states that a notification, whether it be an initial notification or a full notification, must be in writing, and must take the form and manner as determined by the relevant regulator.

h. Paragraph (7) states that a notification under paragraph (2) must also be provided to the CSIRT at the same time as the regulator.

88. A list of factors to which a data centre operator must have regard when determining whether 'significant impact' has had, could have had, is having, or is likely to have occurred, may be introduced through regulations made under **clause 29(1).** This differs to other OES, where the list of factors is stipulated at regulation 11(4).

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

89. Subsection (3) further adds new regulation 11B to the NIS Regulations, which establish the functions of regulators and the CSIRT in relation to notified incidents.

a. Paragraphs (1) and (2) of new regulation 11B set out that the CSIRT, upon receiving a notification under new regulation 11 or 11A, can inform a relevant authority in a country or territory outside the UK if they consider that the incident had, or is likely to have, a significant impact on the operation and security of a network and information system used for essential services in that country or territory. "Relevant authority" is defined for the purposes of these provisions in paragraph (3).

b. Paragraph (4) says that both the regulator and CSIRT may share information with

the regulated entity that issued the notification, where they consider that the information could help the entity to respond to the incident or prevent a future incident.

c. Paragraph (6) states that the regulator or the CSIRT may share information about the incident with the public. The regulator is also given the power to direct the operator to inform the public themselves. However, paragraph (5) provides that paragraph (6) only applies where the regulator or CSIRT, after consulting the notifying OES, considers that public awareness of the incident is necessary to manage the incident or to prevent a future incident, or if it is in the public interest to make the public aware of it.

d. Paragraph (7) establishes that the power to inform the public may only be used once the regulator or CSIRT have consulted each other and the OES who gave the notification.

e. Paragraph (8) states that the regulator can only direct an OES to inform the public about an incident once the regulator has consulted both the CSIRT and the OES in question.

f. Paragraph (9) allows the regulator or CSIRT to disclose information from a notification to either an OES, RDSP, RMSP, or critical supplier, where the regulator or incident response team considers that disclosure is necessary in the interests of preventing other similar incidents.

g. Paragraph (10) specifies that a disclosure of information made under new paragraphs (1), (2) or (9) must not contain any confidential information, or any information that may prejudice the security or commercial interests of an OES.

h. Paragraph (11) specifies that a disclosure of information to the public made under paragraph (6) must not contain any information that may prejudice the security interests of a regulated person.

i. Paragraph (112) establishes that following a disclosure of information under paragraph (9), that information must not be further disclosed without the consent of the regulator or the CSIRT who disclosed it, and, where this relates to an identifiable regulated person, the consent of that regulated person.

j. Paragraph (13) states that a regulator must provide an annual report to the SPOC (single point of contact) identifying the number and nature of incidents reported to it under new regulations 11(2)(b) and 11A(2)(b).

90. Subsection (4) removes paragraphs (3) to (9) and (11) to (16) from regulation 12 of the NIS Regulations.

91. Subsection (5) inserts new regulation 12A to the NIS Regulations, relating to the notification of RDSP incidents. It also adds new regulation 12B, detailing the functions of the Information Commission and CSIRT in relation to notified incidents.

Notification of RDSP incidents

a. Paragraph (1)(a) of new regulation 12A details that, if an RDSP is aware that an RDSP incident has occurred or is occurring, it must send an initial notification to the Information Commission. The initial notification must include the RDSP's name; the digital service to which the incident relates; and brief details of the incident.

b. Paragraph (1)(b) adds that a full notification must also be sent to the Information Commission. The full notification must include the information set out at paragraph (4), but only insofar as that information is known to the RDSP.

c. Paragraph (2) states that an RDSP incident is an incident that has affected, or is affecting, the operation or security of the network and information systems on which the RDSP relies in order to provide the relevant digital service, and has had or is likely to have a significant impact with regard to the factors listed in paragraph (3) in the whole or part of the UK.

d. Paragraph (3) lists factors to which an RDSP must have regard in determining whether an incident has had, is having, or is likely to have a significant impact.

e. Paragraph (4) lists the information that must be included in a full notification, insofar as the information is known to the RDSP. The RDSP must also provide any other information that the RDSP considers may assist the Information Commission in exercising its functions in relation to the incident.

f. Paragraph (5) sets out the timescales in which the notifications must be sent. The initial notification, containing brief details of the incident, must be sent within 24 hours of the RDSP becoming aware of the incident. The full notification must be sent within 72 hours of the RDSP being aware of the incident.

g. Paragraph (6) states that a notification, whether it be an initial notification or a full notification, must be in writing, and must be in the form determined by the Information Commission.

h. Paragraph (7) states that an RDSP must send a copy of a notification to the CSIRT at the same time as sending the notification to the Information Commission.

i. Paragraph (8) establishes that in regulations 12A and 12B, "regulated person" refers to an OES, RDSP, RMSP or critical supplier.

Functions of the Information Commission and CSIRT in relation to notified incidents

92. Subsection (5) also inserts new regulation 12B in the NIS Regulations. It sets out the functions of the Information Commission and the CSIRT in relation to notified incidents.

a. Paragraph (1) of new regulation 12B sets out that the CSIRT, upon receiving a notification under new regulation 12A, can inform a relevant authority in a country or territory outside the UK if they consider that the incident had, or is likely to have, a significant impact on the operation and security of a network and information system used for a relevant digital service in that country or territory.

Relevant authority is defined for these purposes by paragraph (13).

b. Paragraph (2) says that both the Information Commission and the CSIRT may share information with the entity that issued the notification, where they consider that the information could help the entity to respond to the incident or prevent a future incident.

c. Paragraph (4) states that the Information Commission or the CSIRT may share information about the incident with the public. The Information Commission is also given the power to direct the operator to inform the public themselves. However, paragraph (3) clarifies that paragraph (4) only applies where the regulator or CSIRT, after consulting the notifying RDSP, considers that public awareness of the incident is necessary to manage the incident or to prevent a future incident, or if it is in the public interest to make the public aware of it.

d. Paragraph (5) establishes that the power to inform the public may only be used once the Information Commission or CSIRT have consulted each other and the RDSP who gave the notification.

e. Paragraph (6) states that the Information Commission can only direct an RDSP to inform the public about an incident once the Information Commission has consulted both the CSIRT and the RDSP in question.

f. Paragraph (7) allows the Information Commission or CSIRT to disclose information from a notification to either an OES, RDSP, RMSP, or critical supplier, where the Information Commission or incident response team considers that disclosure is necessary in the interests of preventing other similar incidents.

g. Paragraph (8) states that the Information Commission may inform the public about an incident affecting relevant digital services in a country or territory outside the UK if a relevant authority from that country or territory notifies the Information Commission and, after consulting that relevant authority, the Information Commission considers that public awareness of the incident is necessary to manage the incident or to prevent a future incident or is otherwise in the public interest.

h. Paragraph (9) specifies that a disclosure of information made under new paragraph (1) or (7) must not contain any confidential information, or any information that may prejudice the security or commercial interests of an RDSP.

i. Paragraph (10) specifies that a disclosure of information made under new paragraph (4) or (8) must not contain any information that may prejudice the security interests of an RDSP.

j. Paragraph (11) establishes that a disclosure of information under new paragraph (7) must not be further disclosed without the consent of whichever of the Information Commission or the CSIRT disclosed it and, where this relates to an identifiable RDSP, the consent of that RDSP.

k. Paragraph (12) states that the Information Commission must provide an annual report to the single point of contact identifying the number and nature of incidents

reported to it under these regulations.

l. Paragraph (13) sets out when an authority in a country or territory outside the UK is a relevant authority for the purposes of paragraphs (1) and (8).

93. Subsection (6) substitutes “12(3)” for “12A” in regulation 13.

94. Subsection (7) inserts new regulation 14E to the NIS Regulations, relating to the notification of RMSP incidents. It also adds new regulation 14F, detailing the functions of the Information Commission and CSIRT in relation to notified incidents.

Notification of RMSP incidents

a. Paragraph (1)(a) of new regulation 14E details that, if an RMSP is aware than an RMSP incident has occurred or is occurring, it must send an initial notification to the Information Commission. The initial notification must include the RMSP’s name and brief details of the incident.

b. Paragraph (1)(b) adds that a full notification must also be sent to the Information Commission. The full notification must include the information set out at paragraph (4), but only insofar as that information is known to RMSP.

c. Paragraph (2) states that an RMSP incident is an incident that has affected, or is affecting, the operation or security of the network and information systems on which the provider relies in order to provide the managed service, and has had or is likely to have a significant impact with regard to the factors listed in paragraph (3) in the whole or part of the UK.

d. Paragraph (3) lists factors to which an RMSP must have regard in determining whether an incident has had, is having, or is likely to have a significant impact.

e. Paragraph (4) lists the information that must be included in a full notification, insofar as the information is known to the RMSP. The RMSP must also provide any other information that the RMSP considers may assist the Information Commission in exercising its functions in relation to the incident.

f. Paragraph (5) sets out the timescales in which the notifications must be sent. The initial notification, containing brief details of the incident, must be sent within 24 hours of the RMSP becoming aware of the incident. The full notification must be sent within 72 hours of the RMSP being aware of the incident.

g. Paragraph (6) states that a notification, whether it be an initial notification or a full notification, must be in writing, and must take the form and manner as determined by the Information Commission.

h. Paragraph (7) states that an RMSP must send a copy of a notification to the CSIRT at the same time as sending the notification to the Information Commission.

i. Paragraph (8) establishes that, in regulations 14E and 14F, “regulated person” refers to an OES, RDSP, RMSP, or critical supplier.

Functions of the Information Commission and CSIRT in relation to notified incidents

95. Subsection (7) also inserts new regulation 14F in the NIS Regulations. It sets out the functions of the Information Commission and the CSIRT in relation to notified incidents.

    a. Paragraph (1) of new regulation 14F sets out that the CSIRT, upon receiving a notification under new regulation 14E, can inform a relevant authority in a country or territory outside the UK if the team considers that the incident had, or is likely to have, a significant impact on the operation and security of a network and information system used for a managed service in that country or territory.

    b. Paragraph (2) says that both the Information Commission and the CSIRT may share information with the entity that issued the notification, where they consider that the information could help the entity to respond to the incident or prevent a future incident.

    c. Paragraph (4) states that the Information Commission or the CSIRT may share information about the incident with the public. The Information Commission is also given the power to direct the operator to inform the public themselves. However, paragraph (3) clarifies that paragraph (4) only applies where the regulator or CSIRT, after consulting the notifying RMSP, considers that public awareness of the incident is necessary to manage the incident or to prevent a future incident, or if it is in the public interest to make the public aware of it.

    d. Paragraph (5) establishes that the power to inform the public may only be used once the Information Commission or CSIRT have consulted each other and the RMSP who gave the notification.

    e. Paragraph (6) states that the Information Commission can only direct an RMSP to inform the public about an incident once the Information Commission has consulted both the CSIRT and the RMSP in question.

    f. Paragraph (7) allows the Information Commission or CSIRT to disclose information from a notification to either an OES, RDSP, RMSP, or critical supplier, where the Information Commission or CSIRT considers that disclosure is necessary in the interests of preventing other similar incidents.

    g. Paragraph (8) states that the Information Commission may inform the public about an incident affecting a managed service in a country or territory outside the UK if a relevant authority in the affected country or territory notifies the Information Commission and, after consulting the relevant authorities, the Information Commission considers that public awareness of the incident is necessary to manage the incident, prevent a future incident or is otherwise in the public interest.

    h. Paragraph (9) specifies that a disclosure of information made under new paragraph (1) or (7) must not contain any confidential information, or any information that may prejudice the security or commercial interests of a regulated person.

i. Paragraph (10) specifies that a disclosure of information made under new paragraph (4) or (8) must not contain any information that may prejudice the security interests of an RMSP.

j. Paragraph (11) establishes that a disclosure of information under new paragraph (7) must not be further disclosed without the consent of whichever of the Information Commission or the CSIRT disclosed it and, where this relates to a regulated person, the consent of that person.

k. Paragraph (12) states that the Information Commission must provide an annual report to the single point of contact identifying the number and nature of incidents reported to it under these regulations.

l. Paragraph (13) sets out when an authority in a country or territory outside the UK is a relevant authority for the purposes of paragraphs (1) and (8).

Clause 16: Notification of incidents to customers

96. **Clause 16** amends the NIS Regulations to add new requirements for operators of data centres, RDSPs and RMSPs, to send notifications to customers that they consider are likely to have been affected by a reportable incident.

97. Subsection (2) inserts new regulation 11C into the NIS Regulations.

Incidents: notification of customers

a. Paragraph (1) of new regulation 11C sets out that the regulation applies to operators of data centre services.

b. Paragraph (2) specifies that, once the operator of the data centre has given a full notification relating to a data centre incident, it must take reasonable steps to establish which of its customers in the UK are likely to have been adversely affected by the incident as soon as reasonably practicable. It then requires the data centre operator to notify those customers of the incident as soon as reasonably practicable.

c. Paragraph (3) lists the factors that, when considering whether a customer is likely to be adversely affected by the incident, the data centre operator must take into account: the extent of any actual or likely disruption to the provision of the data centre service provided by the OES to the customer; whether the confidentiality, authenticity, integrity or availability of any data relating to the customer is likely to be compromised; and any other impact on network and information systems of the customer.

d. Paragraph (4) states that a notification given by a data centre operator to a customer under this regulation must provide details of the nature of the incident and explain why the data centre operator considers that the customer is likely to be adversely affected by the incident.

98. Subsection (3) inserts new Regulation 12C to the NIS Regulations, setting out provisions for the notification of customers of RDSPs who are likely to be affected by

incidents.

Incidents: notification of customers

a. Paragraph (1) of new regulation 12C specifies that, once the RDSP has given a full incident notification to the Information Commission, it must take reasonable steps to establish which of its customers in the UK are likely to have been adversely affected by the incident as soon as reasonably practicable. It then requires the relevant digital service provider to notify those customers of the incident as soon as reasonably practicable.

b. Paragraph (2) lists the factors that, when considering whether a customer is likely to be adversely affected by the incident, the relevant digital service provider must take into account: the extent of any actual or likely disruption to the provision of the relevant digital service provided by the RDSP to the customer; whether the confidentiality, authenticity, integrity or availability of any data relating to the customer is likely to be compromised; and any other impact on network and information systems of the customer.

c. Paragraph (3) states that a notification given by an RDSP to a customer under this regulation must provide details of the nature of the incident, and explain why the RDSP considers that the customer is likely to be adversely affected by the incident.

99. Subsection (4) inserts new regulation 14G to the NIS Regulations, setting out provisions for the notification of customers of RMSPs who are likely to be affected by incidents.

Incidents: notification of customers

a. Paragraph (1) of new regulation 14G specifies that, once the RMSP has given a full incident notification to the Information Commission, it must take reasonable steps to establish which of its customers in the UK are likely to have been adversely affected by the incident as soon as reasonably practicable. It then requires the RMSP to notify those customers of the incident as soon as reasonably practicable.

b. Paragraph (2) lists the factors that, when considering whether a customer is likely to be adversely affected by the incident, the relevant managed service provider must take into account: the extent of any actual or likely disruption to the provision of the managed service provided by the RMSP to the customer; whether the confidentiality, authenticity, integrity or availability of any data relating to the customer is likely to be compromised; and any other impact on network and information systems of the customer.

c. Paragraph (3) states that a notification given by an RMSP to a customer under this regulation must provide details of the nature of the incident and explain why the RMSP considers that the customer is likely to be adversely affected by the incident.

Chapter 3: Other amendments

Clause 17: Powers to impose charges

100. **Clause 17** amends the NIS Regulations related to the ability of regulators to impose charges to cover the full cost of their regulatory duties. It inserts a new Part 5A into the NIS Regulations to provide a framework for regulators to impose charges on regulated persons and/or recover costs from them, where the costs and fees relate to the discharge of their regulatory duties under the NIS Regulations. New Part 5A is inserted after regulation 20 and comprises new regulations 20A, 20B, and 20C. Regulation 21 of the NIS Regulations is omitted.

Periodic charges under charging schemes

101. New regulation 20A enables regulators to create charging schemes and require regulated entities to pay charges in accordance with them. This will allow regulators to recover costs for the discharge of their functions under the NIS Regulations and is subject to transparency and consultation requirements. This is consistent with precedents from similar regimes.

    a. Paragraph (1) outlines the basis on which a regulator can impose a charge and defines the terms "charging scheme" and “chargeable period”. It specifies that a regulated entity can be imposed a charge if it was regulated by the regulator during both the whole and part of the chargeable period.

    b. Paragraph (2) specifies that NIS regulators can require regulated entities to pay charges under the charging scheme in respect of costs incurred, or expected to be incurred, as a result of carrying out their functions with respect to the NIS Regulations. This can also include costs incurred in establishing the charging scheme before **clause 17** comes into force.

    c. Paragraph (3) sets out what a charging scheme must include. It requires that a charging scheme must specify: the authority’s duties under the NIS Regulations for which a charge is payable, the periods to which the charge relates, either the charge amount or factors and methodologies used for its determination, when and how a charge is to be paid, and the date from which the scheme has effect (this cannot be within 14 days from the day on which the scheme is published).

    d. Paragraph (4) outlines that regulators can recover costs through a charging scheme in relation to the enforcement of their duties under the NIS Regulations. It also allows that charging schemes may set out different rules for setting or calculating charges for different purposes, or to exempt specific groups from charges.

    e. Paragraph (5) establishes that a charge payable by a person under the scheme need not relate to the exercise of functions in relation to that particular person.

    f. Paragraphs (6) provides that a regulator may revise or revoke its charging scheme.

    g. Paragraph (7) provides that a regulator must publish its charging scheme.

h. Paragraphs (8) and (9) introduce a duty for NIS regulators to consult any of the persons that they regulate and consider it appropriate to consult before making or changing a charging scheme. The duty does not apply where the proposed changes are only minor.

i. Paragraph (10) outlines that charges can be imposed by regulators to OES, RDSPs, RMSPs, and those designated under regulation 14H.

Further provision about periodic charges under regulation 20A

102. New regulation 20B makes provision to enable the setting up and management of charges and charging schemes, as well as reporting requirements.

a. Paragraph (1) determines that where charges are calculated based on the turnover of a regulated entity, if there is a disagreement over a turnover amount, the amount calculated by the authority will be the amount used to calculate the charge.

b. Paragraph (2) classifies charges payable as recoverable civil debts. This is in line with existing provisions in the NIS Regulations.

c. Paragraphs (3) and (4) require NIS regulators that are imposing charges under regulation 20A to publish an end-of-cycle statement setting out the information listed in paragraph (4).

d. Paragraph (5) outlines when the end-of-cycle statement should be published.

e. Paragraph (6) defines the terms “chargeable period” and “charging scheme” for the purpose of regulation 20B.

Charges (other than under periodic charges under regulation 20A)

103. New regulation 20C outlines the NIS regulators’ power to recover costs directly for discharging duties under the NIS Regulations.

a. Paragraph (1) permits a NIS regulator to charge for costs incurred by it or on its behalf while performing regulatory functions under the NIS Regulations in relation to a specific person while they were a regulated entity.

b. Paragraph (2) requires the NIS regulators to issue invoices setting out the relevant costs.

c. Paragraph (3) states that a NIS regulator cannot recover charges directly where they are already recoverable under that NIS regulator’s charging scheme or they relate to appeals or civil proceedings under regulations 19A and A20.

d. Paragraph (4) classifies charges payable as recoverable civil debts.

e. Paragraph (5) clarifies that regulated person referred to in this regulation is to have the same meaning as in regulation 20A(10).

Clause 18: Sharing and use of information under the NIS Regulations

104. **Clause 18** amends information sharing provisions under the NIS Regulations to create new information sharing gateways and improve safeguards on how information can be used once it has been shared under the regulations. It specifies conditions and safeguards, entities involved, and the purposes for which information may be shared.

105. Subsection (1) amends wording in regulation 3(3)(e) of the NIS Regulations to amend the purposes for which GCHQ might use lists of designated OESs that it has received from regulators. It also specifies the frequency with which regulators must share the register with GCHQ. This aligns with changes being made to the purposes the Information Commission sharing lists of RDSPs outlined in regulation 6B, subsection (6).

Sharing of information

106. Subsection (2) amends regulation 4 of the NIS Regulations (relating to the functions of the single point of contact or SPOC), substituting "Member State of the EU" for "country or territory outside the United Kingdom" in paragraph (2), and inserting new paragraph (2ZA) setting out which authorities in such a country or territory are to be regarded as relevant authorities for the purposes of this regulation.

107. Subsection (3) replaces the current regulation 6 of the NIS Regulations with new regulations 6, 6A and 6B. New regulation 6 authorises the exchange of information between NIS regulators, the Information Commission and specified entities for purposes related to the functioning of the NIS Regulations, cyber security and resilience and national security.

    a. Paragraph (1) of new regulation 6 provides authorisation for NIS regulators and the Information Commission to disclose information to another regulator and specific entities listed in paragraph (2). It specifies the purposes for which information may be shared.

    b. Paragraph (2) lists the entities, apart from other NIS regulators, that NIS regulators can exchange information with. These are the Secretary of State, relevant law-enforcement authorities, GCHQ, and UK public authorities which are not covered by the above, such as regulators outside of the NIS regime.

    c. Paragraph (3) provides that the entities listed in paragraph (2) can also share information with NIS regulators for the purposes listed in paragraph (1). It also clarifies that 'relevant law enforcement authority' is to be understood as a relevant law enforcement authority which exercises functions within the UK. (Regulation 1(2) of the NIS Regulations provides that "relevant law-enforcement authority" has the meaning given in section 63A(1A) of the Police and Criminal Evidence Act 1984.)

    d. Paragraph (4) requires that disclosures made under paragraphs (1) or (3) must be limited to information that is relevant and proportionate to the purpose for which information is being shared.

    e. Paragraph (5) authorises NIS regulators to disclose information to the Secretary of State if the disclosure is considered to meet the conditions set out in

subparagraphs (a) to (c). These conditions may include the disclosure being relevant to the Secretary of State's role in preparing reports of network and information systems legislation, as required in **clause 40**. The conditions may also include assisting the Secretary of State's assessment of the security and resilience of network and information systems, the provision and availability of data centre services in the UK, and other issues relating to cyber security and resilience (paragraph (5)(b)) or assisting the Secretary of State in formulating policy relating to paragraph (5)(b) and national security.

f. Paragraph (6) provides that the Secretary of State can share information with a NIS regulator if the Secretary of State considers this will assist in preparing reports on network and information systems legislation, assessing anything in paragraph (5)(b) or in formulating policy relating to anything mentioned in paragraph (5)(c).

g. Paragraph (7) provides that NIS regulators may share information they have obtained in the exercise of their functions with a relevant overseas authority if it is shared for one or more of the purposes mentioned in paragraph (1) and the disclosure is limited to information that is relevant and proportionate to the purpose for which the disclosure is being made. "Relevant overseas authority" is defined in paragraph (8) as a person in a country or territory outside the UK appearing to the NIS regulator to exercise functions of a public nature corresponding to those of a NIS regulator, the SPOC or the CSIRT, or which relate to any matters mentioned by paragraphs 1(b) to (e).

h. Paragraph (9) defines the meaning of "data centre service" and "UK public authority" for the purposes of new regulation 6.

Onward disclosure of information and further provision about information sharing

108. New regulation 6A enables and establishes safeguards for the onward sharing of information received by entities under the regulations outlined above and sets out provisions regarding the sharing of confidential information.

a. Paragraph (1) restricts onward sharing of information save for in the circumstances listed in either paragraphs (2) or (4).

b. Paragraph (2) allows for the onward sharing of information to the Secretary of State if the conditions set out in new regulation 6(1) and (4) are met or if the person making the disclosure considers that any of the purposes in sub-paragraphs (a) to (c) of regulation 6(5) apply. It also enables information to be disclosed to the relevant bodies ('persons') listed below in paragraph (3) if the conditions in regulation 6(1) and (4) are met.

c. Paragraph (3) specifies that the 'persons' referred to above are law-enforcement authorities, GCHQ (as the CSIRT), and other UK public authorities.

d. Paragraph (4) allows for onward disclosure of information to any person where there is consent from the person from whom the information was obtained, and consent of an individual or business if the information can identify that individual or business.

e. Paragraph (5) provides that disclosures made under any provision of regulation 6 or this regulation do not breach any obligations of confidentiality that may be owed by the person making the disclosure, or other restriction on the disclosure of information (however imposed). This facilitates the sharing of confidential information, where appropriate, and subject to the limitations in these regulations as well as subject to data protection legislation (see in particular section 183A of the Data Protection Act 2018).

f. Paragraph (6) specifies that nothing in regulation 6 or this regulation authorises information sharing that is prohibited under the relevant sections of the Investigatory Powers Act 2016.

g. Paragraph (7) provides that regulation 6 and this regulation do not limit other provisions that allow the sharing of information under other regulations.

Use of information by the Information Commission

109. New regulation 6B specifies how the Information Commission can use information obtained by it under the NIS Regulations for the purpose of facilitating any of its functions, if it considers that use of the information for that purpose is necessary and proportionate.

110. Subsection (4) applies the ability to share confidential information (in the same way as specified in regulation 6A (5) and 6)) to information sharing in Northern Ireland by amending regulation 7 of the NIS regulations. It also specifies that nothing in regulation 7 authorises information sharing that is prohibited under the relevant sections of the Investigatory Powers Act 2016.

Clause 19: Guidance

111. **Clause 19** amends the NIS Regulations to mandate that regulators publish guidance on the security requirements and incident reporting requirements for OES, RDSPs and RMSPs and for registering with the Information Commission for RDSPs and RMSPs.

112. Subsection (4) inserts new paragraphs (3ZA), (3ZB), and (3ZC).

a. New paragraph (3ZA) requires that guidance issued by regulators must include guidance for OESs on security requirements and the duty to notify incidents.

b. New paragraph (3ZB) provides that when preparing guidance under paragraph (3)(b), a regulator must have regard to any provisions of a code of practice issued by the Secretary of State (per **clause 36**) which are relevant and in force.

c. New paragraph (3ZC) provides that when preparing guidance under paragraph (3)(b) that relates to critical suppliers, or the designation of a person as a critical supplier under new regulation 14H (per **clause 12**), a regulator must coordinate with other regulators with a view to ensuring consistency, and they must consult other regulators before publishing the guidance.

113. Subsection (4) inserts new paragraphs (4A), (4B), and (4C).

a. New paragraph (4A) requires that regulators must publish guidance for RDSPs and RMSPs on security requirements and the duty to notify incidents.

b. New paragraph (4B) provides that when preparing guidance under paragraph (4)(b), the Information Commission must have regard to any provisions of a code of practice issued by the Secretary of State (per **clause 36**) which are relevant and in force.

c. New paragraph (4C) provides that when preparing guidance under paragraph (4)(b) that relates to critical suppliers, or the designation of a person as a critical supplier under new regulation 14H (per **clause 12**), the Information Commission must coordinate with other regulators and the with a view to ensuring consistency, and they must consult other regulators before publishing the guidance.

114. Subsection (5) inserts new paragraph (7) which sets out the definition of "relevant code."

115. Subsection (6) inserts new regulation 3A, which requires regulators to have regard to any relevant guidance published by the Secretary of State when carrying out their functions.

Clause 20: Powers to require information

116. **Clause 20** amends the NIS Regulations with regards to information requirements.

117. Subsection (2) changes the heading of Part 5 of the regulations from "Enforcement" to "Information, enforcement".

118. Subsection (3) substitutes current regulation 15 with new regulation 15, to include the following provisions.

Information gathering

a. Paragraph (1) and (2) set out that a regulator may require a person that fulfils the criteria in new paragraph (3) to give that regulator any information or documents that they reasonably require in order to exercise, or decide whether to exercise, any of their functions under the NIS Regulations.

b. Paragraph (3) clarifies that a regulator can collect information from any person that is regulated by the regulator, or who the regulator considers to be likely to have the information or documents sought.

c. Paragraph (4) and (5) detail some of the reasons for which a regulator might wish to collect information from a person.

d. Paragraph (6) lists the information that must be included in any requirement for information.

e. Paragraph (7) states that, where information is sought from a person not

regulated by the regulator, the information notice may take the form of a general request for information from a group of persons specified in the notice and may be published in a way to bring it to the attention of the persons from whom the information is sought. This power could be used to request information from non-regulated persons in a certain sector with a certain level of turnover, for example.

f. Paragraph (8) states that a person who receives an information notice must comply with its requirements.

g. Paragraph (9) defines, for the purposes of new regulation 15, that a person is regulated by a regulator if it is an OES within the regulator's sector or if it has been designated as a critical supplier by the regulator. A person is regulated by the Information Commission if it is an RDSP; is an RMSP; or has been designated as a critical supplier by the Information Commission.

Information gathering: further provision

119. Subsection (3) also adds new regulation 15A to the NIS Regulations, which contains further provisions about information gathering.

a. Paragraph (1) states that an information notice can require the person in receipt to generate or obtain information and collect or retain information that they may otherwise not have collected or retained.

b. Paragraphs (2) and (3) establish that an information notice can be given to a person outside of the UK, and that the powers are exercisable in relation to information regardless of whether that information is held in the UK or overseas.

c. Paragraphs (4) to (6) determine that an information notice cannot require a person to share legally privileged information with the regulator.

d. Paragraph (7) explains how an information notice can be revoked by the regulator.

Clause 21: Financial penalties

120. **Clause 21** amends the enforcement mechanisms available to regulators to enforce the NIS Regulations. It makes changes to the maximum amount of a penalty, the structure of the penalty banding, and other changes necessary to operationalise and improve the penalty enforcement process.

121. Subsection (2) inserts new paragraphs (2A) and (2B) to regulation 18 of the NIS Regulations.

a. Paragraph (2A) sets out that the Information Commission may serve a notice of intention to impose a penalty on an RMSP if the Information Commission believes the RMSP has failed to comply with relevant duties under the NIS Regulations and a penalty is warranted, having regard to the facts and circumstances of the case.

b. Paragraph (2B) sets out that a NIS regulator may serve a notice of intention to

impose a penalty on a person if the regulator has reasonable grounds to believe that the person failed to comply with an Information Notice served by that regulator, or with the duty set out in regulation 17(3A) (duty to comply with any requirements imposed under an enforcement notice). A notice of intention to impose a penalty can only be served under this paragraph if the regulator considers the penalty is warranted having regard to the facts and circumstances of the case.

122. Subsection (3) substitutes paragraphs (3A) and (3B) of regulation 18 of the NIS Regulations with new paragraphs (3A) and (3B).

a. New paragraph (3A) states that new paragraph (3B) applies where a regulator has served a notice of intention to impose a penalty on a person.

b. New paragraph (3B) establishes that a regulator may serve a final penalty decision once the regulator has considered any representations and still believes a penalty is warranted, having regard to the facts and circumstances of the case.

123. Subsections (4-6) amend paragraphs (3C) to (3E) of regulation 18 to enable regulators to serve notices of intention to impose a penalty and penalty notices on RMSPs, as well as OES and RDSPs.

124. Subsection (7) substitutes paragraphs (5) to (7) of regulation 18 concerning the imposition of financial penalties.

a. New paragraph (5) provides details as to how a regulator can determine an appropriate financial penalty for non-compliance.

i. Subparagraph (a) provides that a penalty imposed under regulation 18 must be of an amount which the regulator determines to be appropriate and proportionate in the circumstances, having particular regard to the factors set out at new paragraph (6).

ii. Subparagraph (b) establishes that the amount must not exceed the maximum amount imposable as set out in paragraphs (7) to (9).

b. Paragraph (6) sets out factors which must be considered when determining the amount of any financial penalty. This is not an exhaustive list, and regulators may consider other factors they deem relevant to the circumstances of the case, attaching such weight to those factors as they see fit (paragraph 6 does not set out the weight to be attached to the factors specified: this will be for regulators to decide based on the facts of the particular case).

c. Paragraph (7) sets out that the maximum penalty for a regulated entity failing to comply with the duties listed in paragraph (10) is subject to the standard maximum amount (defined in paragraph (8)) and failing to comply with the duties listed in paragraph (11) is subject to the higher maximum amount (defined in paragraph (9)).

d. Paragraphs (8) and (9) make provision for the standard and higher maximum

penalty amounts, as referenced in paragraph (7). The standard maximum amount is set at £10,000,000, or 2% of worldwide turnover if the person is an undertaking, whichever is higher; while the higher maximum amount is set at £17,000,000, or 4% of worldwide turnover if the person is an undertaking, whichever is higher. Regulated entities which are not undertakings are therefore subject to maximum penalties of £10,000,000, and £17,000,000 only. **Clauses 29(1)** and **32** give the Secretary of State the power to make regulations about the meaning of undertaking and how turnover is to be calculated for the purposes of these provisions, as well the power to increase turnover-based penalties up to a maximum of 10% of worldwide turnover.

e. Paragraph (10) lists the duties for which a penalty for failing to comply is subject to the standard maximum amount.

f. Paragraph (11) lists the duties for which a penalty for failing to comply is subject to the higher maximum amount.

Clause 22: Enforcement and appeals

125. **Clause 22** sets out that Schedule 1 to this Bill contains further amendments to the enforcement and appeals provisions of the NIS Regulations.

Clause 23: Minor and consequential amendments etc

126. **Clause 23** sets out that Schedule 2 to this Bill contains minor and consequential amendments, both to the NIS Regulations and to other enactments.

Part 3: Security and Resilience of Systems: Functions of the Secretary of State

Chapter 1: Introductory

Clause 24: Key definitions in Part 3

127. **Clause 24** sets out key definitions for the purposes of Part 3 of the Bill, including for any new regulations made under **clause 29(1),** the statement of strategic priorities designated under **clause 25**, and the powers of direction given under **clause 43**. **Clause 24** also includes a new power enabling the Secretary of State to specify new activities, which includes services, that can be brought into scope of the NIS Regulations. Those carrying out these activities (or providing these services) could then be made subject to duties to take proportionate steps to ensure the security and resilience of network and information systems by regulations made under **clause 29(1)**.

128. Subsections (1) and (2) give a definition of “network and information system” for the purposes of Part 3 of the Bill.

129. Subsection (3) defines an “essential activity” as one that is specified by the Secretary of State in regulations. It introduces a new power for the Secretary of State to bring

additional activities into scope of the NIS Regime.

130. Subsection (4) introduces a condition for the power in subsection (3) – with a test for what activities can be bought into scope via regulations. This provides that the Secretary of State can only specify an activity if it is deemed to be essential to the economy of the UK or any part of the UK, or essential to the day-to-day functioning of society in the UK or in any part of the UK.

131. Subsection (5) clarifies that "activity" includes the provision of a service. This means that organisations could be brought into scope if they provide a service or if they carry on another type of activity (such as the production of goods), so long as it means the test set out in subsection (4). Subsection (5) also provides that essential services and relevant digital and managed services (all within the meaning of the NIS Regulations) are to be treated as essential activities for the purposes of Part 3 of the Act.

132. Subsection (6) defines "regulatory authority" as a person specified for the purposes of that subsection by regulations made by the Secretary of State. This would enable the Secretary of State to designate a new regulator where, for example, a new service or other type of essential activity was brought into scope via regulations which could not be appropriately regulated by one of the existing designated regulators.

133. Subsection (7) sets the parameters of which organisations can be designated as regulators by specifying that they must exercise functions of a public nature in the UK.

134. Subsection (8) establishes that existing regulators, as designated by regulation 3(1) of the NIS Regulations, and the Information Commission are to be treated as for the purposes of Part 3 as having been designated under subsection (6).

135. Subsection (9) signposts the definition of "regulated person" (for the purposes of Chapters 3 and 4) is in **clause 30(2).**

Example: bringing more activities into scope

The Secretary of State may deem it appropriate to bring more essential activities into scope of the NIS Regulations. This may be due to increasing reliance on that activity and/or increased threat of cyber attack which could put public services, businesses and/or national security at risk.

The Secretary of State would consult with relevant persons, for instance the organisations that would be brought into scope and the regulator that would be made responsible for overseeing compliance with the Regulations.

The Secretary of State would then make regulations under **clause 24** (in the form of a statutory instrument) specifying the new activity and, where appropriate, designating a new regulator**.**

Regulations made at the same time by the Secretary of State under **clauses 29 – 31** could then designate persons carrying out the newly specified service or other activity as regulated persons. They could also amend the NIS Regulations 2018 in order to bring this new category of regulated persons within the scope of the duties and requirements existing with that regulatory regime.

Alternatively, the **clause 29** power could be used to establish a new, separate regulatory regime for this new category of regulated persons. Regulations made under **clauses 24(3)** and **29(1)** could be combined in a single instrument, subject to the affirmative procedure.

Chapter 2: Statement of Strategic Priorities etc

Clause 25: Statement of strategic priorities etc

136. Subsections (1) and (2) of **clause 25** introduce a power for the Secretary of State to designate a statement of the government's strategic priorities in relation to the security and resilience of network and information systems relevant to the carrying on of essential activities. It adds that, alongside priorities, the statement must set objectives for regulators relating to the priorities and must set out the roles and responsibilities of different organisations in relation to the priorities. The power is similar to existing powers to issue statements of strategic priorities that the Secretary of State has in the Online Safety Act 2023 and the Communications Act 2003.

137. Subsection (3) requires that the designated statement must be published in a manner that the Secretary of State considers appropriate.

138. Subsection (4) establishes that a designated statement can be amended, including by being replaced in full. Subsection (5) states that a statement designated under subsection (1) may be withdrawn by the Secretary of State.

139. Subsection (6) clarifies that a statement cannot be withdrawn or amended within three years of it having been designated, unless the criteria set out in subsection (7) are met.

140. Subsection (7) says that an amendment to, or withdrawal of, a statement can be made sooner than three years after its designation if there has been a general election, or if the Secretary of State considers that there has been a significant change in government policy or threat landscape in relation to the security and

resilience of network and information systems relied on in connection with the carrying on of essential activities.

141. Subsection (8) states that corrections to the drafting of the statement, such as to correct misspellings of words, can be made without it constituting an amendment to the designated statement.

Clause 26: Consultation and procedure in relation to statement

143. **Clause 26** sets out the consultation and parliamentary procedure requirements that must be satisfied before the Secretary of State can designate a statement of strategic priorities.

144. Subsection (1) explains that this section lists the steps that must be taken before a statement of strategic priorities is able to be given legal effect.

145. Subsection (2) establishes that the Secretary of State must consult the NIS regulators on a draft of the proposed statement. Regulators must be afforded at least 40 days within which to provide comments on the proposed draft, as set out at subsection (3).

146. Following this period of consultation, subsection (4) states that the Secretary of State must make any changes to the draft statement that appear appropriate to the Secretary of State as a result of the consultation. The Secretary of State must then lay the statement before Parliament.

147. Subsections (5) to (7) outline parliamentary procedure and specifies that the draft statement will be subject to the same procedure as a Statutory Instrument which is subject to the negative resolution procedure. After that procedure, the Secretary of State may designate the final statement.

148. Subsection (8) sets out that the consultation process detailed in subsections (2) and (3) could be undertaken before the coming into force of **clause 25**, including consultation undertaken before the passing of this Bill.

Clause 27: Duties of regulatory authorities in relation to statement

149. **Clause 27** introduces requirements on regulators in relation to the designated statement of strategic priorities.

150. Subsection (1) sets out that regulators will have duties related to a statement for the period that it has been designated by the Secretary of State.

151. Subsection (2)(a) sets out that regulators are to have regard to the statement whilst carrying out their regulatory functions.

152. Subsection (2)(b) adds that regulators are also required to exercise their functions in a manner that seeks to achieve any relevant objectives included in the statement.

153. Subsection (3) specifies that these duties apply to regulators' functions insofar as they are derived from the NIS Regulations or from Part 3 and Part 4 of this Bill.

Clause 28: Report by Secretary of State

154. **Clause 28** sets out the reporting requirements for a Statement of Strategic Priorities issued by the Secretary of State.

155. Subsection (1) of this clause requires the Secretary of State to lay before Parliament a regular report setting out, in general terms, the steps that regulators have taken in the reporting period to meet the duties set out in **clause 27** and the steps that regulators plan to take in the next reporting period in relation to those same duties.

156. Subsection (2) requires that the report must also be published in a manner that the Secretary of State deems appropriate.

157. Subsection (3) establishes that the “reporting period” to be covered in the Secretary of State’s report refers to the period of 12 months following the designation of the statement, and every 12-month period following.

158. Subsections (4) and (5) set out that the Secretary of State may require a regulator to provide information for the purposes of compiling the report, through the issuing of an information notice. A regulator in receipt of an information notice must provide the information by the deadline and in the format specified by the notice.

Chapter 3: Regulations about security and resilience of systems

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

159. Subsection (1) of **clause 29** grants the Secretary of State powers to make regulations which can add to, amend or replace the existing NIS Regulations. It specifies that regulations can be made with the objective of identifying, managing and reducing the risks, and mitigating the adverse impacts of security or operational compromises to network and information systems (including actions related to remediation).

160. Subsection (2) sets that that the objectives in subsection (1) may include provision for strengthening the resilience of networks and information systems, including their physical environments.

161. Subsections (3) and (4) defines a “relevant” network and information system for the purposes of this chapter, with further explanation given for when a system is considered “associated” with another.

162. Subsection (5) and (6) clarify what is meant by the terms "security or operational compromise," and “service-critical supply” within the Chapter.

Example:

The NIS Regulations contain a set of duties in relation to the management of risk to network and information systems for essential and digital services, and the expectations for complying

with these duties are set by regulators in guidance. The Secretary of State may, by regulations, add further detail for those security duties. This could include, for example, mandatory steps to strengthen the resilience of relevant network and information systems and their surrounding environment, in order to mitigate particular risks from emerging technologies.

Clause 30: Imposition of requirements on regulated persons

167. Subsection (1) of **clause 30** expands on the extent of the power for the Secretary of State to make regulations for the purpose of protecting network and information systems, providing that regulations made under **clause 29(1)** can impose requirements on regulated persons. The following subsections give further detail to what requirements the regulations made under **clause 29(1)** can impose on regulated persons.

168. Subsection (2) and (3) defines "regulated persons" for the purposes of Chapter 3. A regulated person is a person specified, or of a description specified, for the purposes of subsection (2) in regulations made by the Secretary of State. A person (or description) may only be specified in regulations if the person (or every person of the description) carries on an essential activity in the UK or provides an activity-crucial supply. A description of persons carrying on an essential activity could, for example, be all persons carrying on that activity or a sub-set of such persons.

169. Subsection (4) clarifies that the specification of a person or description of persons under subsection (2) can be framed by reference to whether that person or description of persons is for the time-being designated by a regulator in accordance with regulations made under **clause 29(1)**. For example, regulations made by virtue of subsection (2) could specify as “regulated persons” any person carry on a specific type of essential activity and who is for the time-being designated by a particular regulator in accordance with regulatory provision made under **clause 29**. In this case, the regulator’s designation decision would determine whether a particular person was subject to regulation as a “regulated person”.

170. Subsection (5) clarifies that OESs, RDSPs, RMSPs and critical suppliers are treated as ‘regulated persons’ for the purposes of subsection (2).

171. Subsection (6) provides a non-exhaustive list of specific requirements that may be imposed on regulated persons. It provides that such duties can include taking specified measures aimed at achieving objectives related to reducing and mitigating cyber security risks and impacts, as established by **clause 29(1),** including measures outside the UK as well as requirements in the form of prohibitions or restrictions**.** Additionally, it may encompass requirements regarding the reporting of certain matters, disclosing information to regulators and other persons, and appointing representatives within the UK (in the case of regulated persons established outside the UK).

172. Subsection (7) outlines that “specified” means specified in regulations under **clause 29(1).**

Clause 31: Functions of regulatory authorities: enforcement, sanctions and appeals

173. **Clause 31** also expands on the power for the Secretary of State to make regulations for the purpose of protecting network and information systems, setting out that the regulations made under **clause 29(1)** may confer functions on regulators in connection with compliance with the regulations.

174. Subsection (1) outlines the functions that the regulations may confer upon regulators. These are functions in connection with monitoring and securing compliance with relevant requirements, investigating suspected non-compliance with relevant requirements and mitigating the effects of non-compliance with relevant requirements.

175. Subsection (2) defines a "relevant requirement" as a requirement imposed by or under regulations made under **clause 29(1)** or the NIS Regulations.

176. Subsection (3) provides a non-exhaustive list relating to the powers and functions that may be conferred on regulators.

177. Subsection (4) states that regulations made under **clause 29(1)** may include conditions related to the exercising of the power conferred. For instance, regulators may be required to produce evidence of their identity or authority before exercising their powers, or they may need to obtain a warrant from a designated individual before entering premises.

178. Subsection (5) clarifies that the regulations made under c**lause 29(1)** may include measures for imposing sanctions, including financial penalties, against those who fail to comply with relevant duties.

179. Subsection (6) requires regulations made under **clause 29(1)**, where they provide for financial penalties, to make provision for appeals. It also sets out that the regulations made under **clause 29(1)** may make provision for appeals for other decisions or actions, separate to financial penalties.

180. Subsection (7) provides a non-exhaustive list of the types of provisions that could be made in reliance to subsection (6).

181. Subsection (8), in reference to subsection (7)(d) sets out what powers a court or tribunal has where an appeal is made to them.

Clause 32: Provision about financial penalties

182. **Clause 32** sets out what can be included in regulations about financial penalties made under **clause 29(1).**

183. Subsection (1) sets out what may, and what must, be included in provisions about financial penalties made by regulations under **clause 29(1)**. It establishes that any provision relating to financial penalties must provide for how the regulator deals with sums received as a result of a penalty, and may also specify penalty amounts, including provision on determinations of amounts, as well as provision on penalty recovery.

184. Subsection (2) clarifies that those provisions can provide for penalties to be determined by reference to a daily rate.

185. Subsection (3) specifies that where provision about penalties is made under **clause 29 (1)**, it must include provision on the maximum penalty that can be imposed by such provision for an undertaking, which can be no more than the greater of £17,000,000 and 10% of worldwide turnover of the undertaking, and may include provision on the maximum amount of penalty for a person who is not an undertaking, which cannot be more than £17,000,000.

186. Subsection (4) adds further detail to about what regulations including provision within subsection (3) may make provision for. This includes provision relating to the meaning of undertaking, and about how turnover is to be calculated.

187. Subsection (5) allows the Secretary of State to make regulations to amend the maximum penalty of £17,000,000 for undertakings and/or non-undertakings for the purpose of reflecting inflation.

Clause 33: Regulatory authorities and other persons: information, guidance and other functions

188. **Clause 33(1)** sets out that regulations may give functions to regulators in relation to disclosure of information, production of guidance and reports, keeping records and the consultation and cooperation with other bodies (including persons outside the UK).

189. Subsection (2) adds more detail about what may be included in regulations made under subsection (1)(a) about the disclosure of information.

190. Subsection (3) clarifies that the regulations may provide for information processed in accordance with regulations not to be in breach of any obligation of confidence owed by the person processing the information, or any other restrictions.

191. Subsection (4) qualifies subsection (3), with the effect that regulations made under **clause 29(1)** requiring or authorising the disclosure of information cannot overrule certain prohibitions on disclosure contained in the Investigatory Powers Act 2016.

192. Subsection (5) sets out that the regulations may place functions on persons who exercise public functions but are not regulators. This could include, for example, conferring additional functions on these authorities.

193. Subsection (6) provides a non-exhaustive list of what these functions could entail.

Clause 34: Recovery of costs of regulatory authorities

194. **Clause 34(1)** sets out that the regulations can enable regulators to impose charges on regulated persons in order to fund their functions under the Regulations.

195. Subsection (2) defines “relevant costs” as any costs incurred by regulators from carrying out their functions conferred by this Part or Part 4, or under the NIS Regulations, including costs in connection with enforcing the requirements imposed with those regulations.

196. Subsection (3) provides that regulations may provide for the imposition of charges in accordance with a scheme made by the authority (a “charging scheme”).

197. Subsection (4) clarifies what may be included in provisions made by regulations under Subsection (1), or in charging schemes authorised by regulations under Subsection (1).

198. Subsection (5) enables the regulations, or charging schemes authorised by the regulations, to impose charges (or the amount of such charges) on a person that are not limited to the costs associated with the regulation of that particular person.

199. Subsection (6) establishes that provisions made under subsection (4)(c) may include provision about deficits incurred by a regulatory authority.

200. Subsection (7) allows regulations made under subsection (1) to authorise a charging scheme to make different provisions for different purposes.

201. Subsection (8) confirms the meaning of ‘relevant requirement’, which is the same as in **clause 31**.

Clause 35: Supplementary provision and interpretation

202. **Clause 35** adds supplementary detail on what regulations made under **clause 29(1)** may do.

203. Subsection (2) makes definitions for the purposes of the Chapter.

Chapter 4: Code of practice

Clause 36: Code of practice

204. **Clause 36** sets out that the Secretary of State may issue a code of practice for regulated persons describing steps recommended to enable compliance with duties, requirements imposed on them, including under regulations made under **clause 29(1)** or the NIS Regulations.

205. Subsection (2) outlines that the Secretary of State is permitted to revise and reissue the code from time to time.

206. Subsection (3) specifies that, before preparing or revising the code, the Secretary of State is required to consult with such persons as deemed appropriate.

207. Subsection (4) stipulates that the code may contain different provisions for different purposes, including variations for different categories of regulated persons as well as transitional or saving provisions.

208. Subsection (5) clarifies that “regulated person” is the same as in **Chapter 3.**

Clause 37: Procedure for issue of code of practice

209. **Clause 37** outlines the procedural requirements for issuing and amending the code of practice.

210. Subsection (1) establishes that, before the Secretary of State issues or reissues a code of practice under **clause 36**, a draft of the proposed code must be laid before Parliament.

211. Subsection (2) specifies that if either House of Parliament resolves not to approve the draft code within the 40-day period, the Secretary of State must not issue the code in the form of that draft. The Secretary of State could prepare another code, which would be subject to the same scrutiny process.

212. Subsection (3) confirms that, should no resolution be passed within the 40-day period, the Secretary of State may proceed to issue or reissue the code of practice.

213. Subsection (4) specifies that the Secretary of State must publish a code that is issued or reissued, with the code coming into effect at the time of publication unless it specifies otherwise.

214. Subsection (5) and (6) specifies how the 40-day period is to be calculated.

215. Subsection (7) grants the Secretary of State the power to make regulations to change the procedure for issuing the code set by amending **clause 36 (1)** to **(6)** so far as it relates to consultation and amending **clause 37** other than this subsection.

Clause 38: Effects of code of practice

216. **Clause 38** clarifies how the code of practice will be used and treated in legal and regulatory settings.

217. Subsection (1) clarifies that failure to follow the code of practice as set out in **clause 36** does not in itself evidence a failure to comply with the requirements to which it relates or make a regulated person liable to legal proceedings in court or tribunal.

218. Subsection (2) clarifies that a code of practice, as set out under **clause 36**, can be used as evidence in legal proceedings. This means that, whilst a regulated person's failure to follow the code of practice does not alone make them liable to legal action, as is set out in subsection (1), failure to follow the code of practice can be accepted as evidence to inform a decision in legal proceedings.

219. Subsection (3) specifies that in any legal proceedings the court or tribunal must consider a code of practice issued under **clause 36** as evidence in proceedings if it was in force at the time of the issue being considered and appears to be relevant.

220. Subsection (4) sets out that a regulator must consider a provision of a code of practice issued under **clause 36** when assessing compliance with requirements under **clause 29(1)** or the NIS Regulations if that provision of the code was active at the time the duties applied and appears to the regulator to be relevant.

Clause 39: Withdrawal of code of practice

221. **Clause 39** allows the Secretary of State to withdraw the code of practice and sets out the process for doing so.

222. Subsection (2) establishes that before the code of practice is withdrawn, the Secretary of State must consult in advance with such persons as the Secretary of State considers appropriate on the proposal to withdraw the code.

223. Subsection (3) establishes that if the Secretary of State decides to withdraw the code of practice they must lay before Parliament notice of the withdrawal of the code.

224. Subsection (4) specifies that withdrawal of a code has effect at the end of the 40-day period, unless the notice of the withdrawal of the code laid before Parliament in Subsection (3) specifies a different timeframe. The notice can also set different end dates for different purposes, and it can include exemptions to keep some parts of the code in effect.

225. Subsection (5) clarifies that the definition of the 40-day period is the same as in **clause 37**.

Chapter 5: Report on network and information systems legislation

Clause 40: Report on network and information systems legislation

226. **Clause 40** sets out requirements for the Secretary of State to report on the operation of network and information systems legislation.

227. Subsection (1) requires the Secretary of State to, at least once every five years, lay a report on the operation of certain network and information systems legislation before parliament and publish it.

228. Subsection (2) defines what is meant by the review period in this clause.

229. Subsection (3) clarifies the range of legislation that should be included in the report as long as it was in force during the reporting period.

230. Subsection (4) outlines the particular content that a report must include.

231. Subsection (5) grants the Secretary of State the power, via regulations, to amend the required content of the reports.

232. Subsection (6) enables the Secretary of State to request information from regulators for the purposes of producing the report, which the regulators are required to provide.

Chapter 6: Regulations under Part 3

Clause 41: Regulations under Clause 24 or Chapter 3

233. **Clause 41** gives further detail on what regulations made under **clause 24** and Chapter 3 of Part 3 may contain.

234. Subsection (1) lists several types of provision that regulations under **clause 24** and Chapter 3 of Part 3 may contain.

235. Subsection (2) provides a definition of ‘relevant UK waters’.

236. Subsection (3) establishes that consequential provisions made under this section may appeal or repeal provisions made by primary legislation.

237. Subsection (4) provides a definition of ‘primary legislation’ for the purposes of this section.

Clause 42: Consultation and procedure

238. **Clause 42** sets consultation requirements and parliamentary procedure for regulations made under the provisions of this Chapter.

239. Subsections (1) and (2) set out a list of regulations which the Secretary of State must consult such persons as the Secretary of State considers to be appropriate before making.

240. Subsection (3) clarifies that the duty to consult on regulations made under subsections (1) and (2) can be satisfied by consultation taking place before the coming into force of **clause 42** (including before the passing of the Bill).

241. Subsections (4), (5) and (6) concern the parliamentary procedure of the regulations made under this Part. Subsection (4) requires any provision made under this Part to be made by statutory instrument. Subsection (5) makes clear that the affirmative procedure will be followed where there is a duty to consult under Subsection (1) or if the regulations amend primary legislation. For all other regulations, the negative procedure will be used.

Part 4: Directions for national security purposes

Clause 43: Directions to regulated persons

242. **Clause 43** grants the Secretary of State the power to issue a direction to a regulated person; sets out the circumstances in which a direction could be issued; the content that should be included in a direction; and the circumstances where disclosure of a direction or consultation may be restricted.

243. Subsection (1)(a) grants the Secretary of State the power to issue a direction to a regulated person if they consider that a security or operational compromise in relation to a relevant network and information system, or the threat of such a compromise, poses a national security risk.

244. Subsection (1)(b) establishes that a direction must be necessary and proportionate in the interests of national security. To decide whether the direction was necessary, the Secretary of State would be expected to assess whether there were any other means to address the national security threat. An assessment of the proportionality of a direction might require the Secretary of State to consider, among other things, the economic impact of issuing the direction, the expected costs of complying with the direction, whether a direction would conflict with any regulatory duties the recipient is subject to, and whether the direction could have any harmful consequences.

245. Subsection (2) sets out that directions may require or prohibit specific actions.

246. Subsection (3) provides a non-exhaustive list of the types of requirements that may be imposed by a direction.

247. Subsection (4) clarifies that, for the purposes of the subsection (1) power, it does not matter whether the risk to national security arising from the occurrence or threat of occurrence of an operational or security compromise relates itself to the carrying on of an essential activity (or the provision of an activity-critical supply) or relates to something else. This means that a direction could be issued, for example, if there was suspected data exfiltration on a network or information system used in connection with the carrying on of an essential activity which gave rise to a national security risk, even if the Secretary of State does not believe that the exfiltration of data would disrupt or otherwise affect the continuity of the carrying on of the essential activity.

248. Subsection (5) lists the information that must be included in a direction. This includes the reasons for the direction, except if or to the extent that the Secretary of States considers it would be contrary to the interest of national security to do so.

249. Subsection (6) requires a person subject to a direction to comply with it.

250. Subsection (7) says that a person in receipt of a direction cannot appoint a skilled person to help it comply with the direction unless the Secretary of State has approved the appointment. It further adds that the entity must notify the Secretary of State as soon as practicable once a skilled person has been appointed.

251. Subsection (8) states that the Secretary of State may refer to a list of skilled persons published by GCHQ to decide whether to provide the approval required under subsection (7)(a).

252. Subsections (9) and (10) require the Secretary of State, before issuing a direction, to consult with the person or persons subject to the direction and other persons the Secretary of State considers appropriate. Other persons consulted could include, for example, the Secretary of State responsible for the sector in which the person proposed to receive the direction operates, or the person's relevant NIS regulator. The requirement to consult only applies insofar as consultation is practicable, and where a consultation would not be contrary to the interests of national security.

253. Subsection (11) allows the Secretary of State to require a person subject to a direction not to disclose the existence or contents of a direction without the permission of the Secretary of State. It also allows the Secretary of State to require a person consulted under subsection (9) not to disclose the existence of a consultation nor the information disclosed as part of the consultation, without the permission of the Secretary of State.

254. Subsection (12) sets out that the Secretary of State may not impose a requirement under subsection (11) – not to disclose the direction or consultation – unless the Secretary of State believes that the restriction of disclosure is necessary and proportionate in the interests of national security.

Example:

A hostile actor is assessed to be present on the networks of an operator of an essential service. The actor is using 'living off the land' techniques to evade detection – i.e., techniques allowing attackers to operate discreetly, with malicious activity blending in with legitimate system and network behaviour making it difficult to differentiate, even by organisations with more mature security postures. The identity of the state actor, and the nature of their compromise of and presence on, the operator of an essential service's networks, creates an ongoing national security risk because this access might provide means for the state actor to disrupt the operation of the essential service at a future date.

In such a situation, the Secretary of State might consider using the Power of Direction to mandate that the operator of an essential service take specified action to confirm the presence of the state actor on the network and, if necessary, remediate. This direction would be subject to an assessment of whether the proposed directed action is necessary and proportionate.

Clause 44: Compliance with directions under section 43 to take priority

255. **Clause 44** outlines that, where a requirement within a direction conflicts with a regulatory obligation to which the person receiving the direction is subject, the Secretary of State can notify the person, in which case compliance with the direction takes precedence over compliance with the other obligation.

256. Subsections (1) and (2) set out that where a requirement imposed by a direction issued under **clause 43** conflicts with one or more of the receiving entity's regulatory duties, and the Secretary of State notifies the person or person of this conflict, the regulatory duty or duties do not apply while the requirement in the direction remains in place.

257. Subsection (3) requires the Secretary of State to notify the relevant regulatory authority where a regulated person or persons is not required to comply with a conflicting regulatory duty, unless it would be contrary to the interests of national security (subsection (5)).

258. Subsection (4) defines "relevant regulator" as a person that may exercise a regulatory function (as defined in the Legislative and Regulatory Reform Act 2006) in relation to the person or persons subject to the direction, and the conflicting requirement.

259. Subsections (6) and (7) outline that, if a direction is revoked or varied under the powers in **clause 54** to remove the previously conflicting requirement, the person or persons that are or were subject to the direction must comply with the previously conflicting regulatory duty as soon as reasonably practicable after being notified of the revocation or variance. The Secretary of State must notify the person or persons subject to the direction and the relevant regulator of the variance or revocation.

260. Subsection (8) states that, in this section, "enactment" includes an enactment comprised in, or an instrument made under, an Act of the Scottish Parliament.

Clause 45: Monitoring by regulatory authorities

261. **Clause 45** gives the Secretary of State the power to delegate the monitoring of compliance with a direction to a regulator. Regulators may be directed to request information relating to compliance and report this information to the Secretary of State. This section also makes provision for the Secretary of State to disclose these reports.

262. Subsection (1) enables the Secretary of State to direct a regulator to obtain information relating to a person's compliance with a direction given to it. The Secretary of State can require the regulator to prepare and send a report to the Secretary of State based on the information collected, or to send the information on which the report is based. The regulator will be engaged in information collection and provision only. The Secretary of State will be responsible for compliance decisions.

263. Subsection (2) sets out the nature of the information which a regulator may be required to obtain under subsection (1). This is limited to information that would assist the Secretary of State in making an assessment regarding compliance with a direction.

264. Subsection (3) states that a regulator which receives a monitoring direction must comply with it.

265. Subsection (4) specifies what may be contained within a direction issued under **clause 45**.

266. Subsection (5) requires a regulator to use their powers under **clause 46(2)** to obtain information in an appropriate manner for the purposes of preparing a report under this section.

267. Subsection (6) allows the Secretary of State to vary or revoke a monitoring direction. Before varying or revoking a monitoring direction, the Secretary of State must consult the regulator subject to the direction (subsection (7)).

268. Subsections (8) and (9) state that, while the Secretary of State cannot issue a direction to another Minister of the Crown or a part of a devolved government, the Secretary of State can request that the minister or devolved government collect compliance information from a person in receipt of a direction, and provide this information or a report based on it to the Secretary of State.

269. Subsection (10) allows the Secretary of State to disclose a report made by a regulator as part of a monitoring direction. The Secretary of State must have regard to the need to exclude from disclosure, as far as practicable, information that could seriously and prejudicially affect to a person's interests (subsection (11)).

Clause 46: Information gathering

270. **Clause 46** gives the Secretary of State and regulators the power to issue an information notice to require a person to provide information which is reasonably required to exercise the functions granted in this Chapter.

271. Subsection (1) grants the Secretary of State the power to require a regulated person to provide information which the Secretary of State reasonably requires to exercise, or

decide whether to exercise, any of the Secretary of State's functions granted by this Part of the Bill.

272. Subsection (2) grants the power for a relevant regulator to require a regulated person to provide information that the relevant regulator requires to comply with a monitoring direction or request issued under **clause 45**.

273. Subsection (3) specifies that a regulated person must be given a notice in writing (an "information notice") when being requested to provide information under subsection (1) or (2).

274. Subsection (4) sets out what an information notice must contain.

275. Subsection (5) provides that a power under subsection (1) or (2) to require a regulated person to give information includes the power to require a regulated person to generate or obtain information and to collect or retain information that would not be collected or retained otherwise, for the purpose of providing the information to the Secretary of State or relevant regulator.

276. Subsection (6) states that a regulated person to whom an information notice is given must comply with the information notice. The powers granted in this section are exercisable in relation to information within or outside the United Kingdom (subsection (7)).

277. Subsections (8), (9) and (11) state that a regulated person may not be required by an information notice to provide privileged communication to the Secretary of State or the relevant regulator. This includes definitions of what constitutes "privileged communication".

278. Subsection (10) states that an information notice given to a regulated person may be revoked by the person who gave the information notice giving a notice to the regulated person.

279. Subsection (12) states that the Secretary of State may not issue an information notice to the CSIRT or the SPOC.

Clause 47: Inspections

280. **Clause 47** gives the Secretary of State and regulators the power to carry out inspections to assess compliance with a direction or a confirmation decision. The Secretary of State and regulators are also able to appoint a person to carry out an inspection on their behalf.

281. Subsection (1) sets out the definition of "inspection".

282. Subsection (2) grants the Secretary of State the power to carry out an inspection, appoint a person to carry out an inspection on behalf of the Secretary of State, or direct a regulated person to appoint a person approved by the Secretary of State to carry out an inspection.

283. Subsection (3) grants a regulator subject to a monitoring direction or request the power to carry out an inspection, appoint a person to carry out an inspection on behalf of the regulator, or direct a regulated person to appoint a person approved by the regulator to carry out an inspection.

284. Subsection (4) lists requirements that a regulated person subject to an inspection under subsection (2) or (3) must follow – including providing the inspector with access to their premises and generally co-operating with the inspector.

285. Subsection (5) specifies that, before carrying out an inspection, the inspector must make the entity to whom the inspection relates aware of the possible consequences if they fail to comply with the inspection.

286. Subsection (6) allows the inspector to enter the premises of a regulated person at any reasonable time, if the inspector has reasonable grounds to believe that entry to the premises may be expedient for the inspection and that the premises is not used as a private dwelling.

287. Subsection (7) requires that the inspector must, if asked by a person on the premises, produce evidence of their identity and outline the purpose of the inspection before entering any premises.

288. Subsection (8) lists the actions that an inspector may take for the purposes of the inspection.

289. Subsection (9) states that a person may not be required to produce or provide an inspector with access to a privileged communication.

290. Subsection (10) specifies that the powers granted by this clause are not exercisable in relation to premises, material, equipment or individuals outside the UK, but they are exercisable in relation to documents or information whether stored within or outside the UK.

291. Subsection (11) defines “inspector” as any person carrying out all or part of an inspection in accordance with this clause.

Clause 48: Notification of contravention

292. **Clause 48** gives the Secretary of State and the regulators the power to issue a notification of contravention where there are reasonable grounds to suspect a person has not complied with requirements as set out in this Part.

293. Subsection (1) allows the enforcement authority to issue a notification of contravention to a person where there are reasonable grounds to suspect the provider person has contravened a “relevant requirement”.

294. Subsection (2) defines a “relevant requirement” and “enforcement authority”.

295. Subsection (3) outlines what a notification of contravention must contain, including any penalties that the enforcement authority may impose of the requirements in the notification of contravention are not met.

296. Subsection (4) states that a notice of contravention can be given in respect of more than one contravention, and that where this is the case, a separate penalty may be specified for each contravention.

297. Subsection (5) provides that, where a contravention is continuing, a notification may be given for any period during which the contravention occurred and no more than one penalty in relation to that contravention for that period may be included in the notice of contravention in line with subsection (3)(e).

298. Subsection (6) provides that in addition to, or instead of, imposing a penalty for a continuing contravention for a set period, a notice of contravention may also include daily penalties that the enforcement authority is minded to impose in relation to a continuing contravention. The daily penalties will only begin accruing after either: a confirmation decision has been issued in line with **Clause 50** and that decision includes a requirement that must be complied with immediately; or a confirmation decision has been issued and a deadline has passed for complying with a requirement in the decision.

299. Subsection (7) provides the circumstances for which an enforcement authority may give a further notification of contravention in respect of the same contravention.

300. Subsection (8) states that, for the purposes of this section, conduct that constitutes or causes a contravention of a relevant requirement can take place in the UK or elsewhere.

301. Subsections (9) and (10) allow the enforcement authority to require a person subject to a notification under this section not to disclose the existence or contents of the notification without the permission of the authority if the Secretary of State considers that disclosure would be contrary to the interests of national security.

Clause 49: Penalty amounts

302. **Clause 49** outlines the penalties that can be imposed for non-compliance and grants the Secretary of State the power to make regulations to define the calculation of turnover for penalties.

303. Subsection (1) requires a penalty specified under **clause 48** to be appropriate and proportionate.

304. Subsection (2) sets out the maximum penalties for contraventions other than daily penalties. An entity that is not an undertaking, would include, for example, an NHS trust. In the case of a contravention by an undertaking of a requirement imposed under a direction issued under **clause 44**, the penalty amount may not exceed the higher of £17 million or 10% of the turnover of the undertaking. In any other case of a contravention of a requirement under **clause 43**, the penalty amount may not exceed £17 million. In the case of a contravention of a requirement to give information under **clause 46(1)** or **46(2**), or a contravention of a requirement relating to an inspection

under **clause 47(2)(c)**, **clause 47(3)(c)** or **clause 47(4)**, the penalty amount may not exceed £10 million.

305. Subsection (3) sets out the maximum daily penalties for continuing contraventions. For contravention under of a requirement imposed by a direction under **clause 43**, and subject to subsection (2), the maximum is £100,000 per day. For a contravention of a requirement to give information under **clause 46(1)** or **46(2)**, the maximum is £50,000 per day, subject to subsection (2).

306. Subsection (4) states that when issuing a daily penalty, no account can be taken of the days before a notice of contravention is served. The date on which a daily penalty begins accruing is set out in **clause 48(6)**. This subsection also states that the daily penalty stops accumulating on the day on which the person first complies with the requirement specified or earlier if determined by the enforcement authority.

307. Subsection (5) requires the Secretary of State to set out, in regulations, the meaning of "undertaking" and the method through which an undertaking's turnover is to be determined.

308. Subsection (6) lists provisions that could be included in regulations under subsection (5), including that, in a case where an undertaking is a member of a group, other members of the group could be treated as part of the undertaking for the purposes of determining the undertaking's turnover.

309. Subsection (7) allows for the Secretary of State to amend the maximum penalty amounts set out in this section in line with inflation by way of regulations.

310. Subsection (8) states that regulations under subsections (5) or (7) may make different provisions for different areas and purposes, and could make consequential, supplementary, incidental, transitional, or saving provision. Subsection (9) adds that regulations under subsections (5) and (7) are subject to the negative procedure.

Clause 50: Enforcement of notification

311. **Clause 50** gives enforcement authorities the power to issue confirmation decisions where a person has been given a notification of contravention under **clause 48**, and where the enforcement authority is satisfied that non-compliance has taken place. The confirmation notice sets out the final decision and can require a penalty to be paid.

312. Subsections (1) and (2) provide that, where a person has been given a notification of contravention under **clause 48** and the period for making representations has expired, the enforcement authority may give the person a confirmation decision, which either confirms the imposition of the requirements set out in the notification, or informs the person that no further action will be taken.

313. Subsection (3) provides that a confirmation decision can only be given if the enforcement authority is satisfied that the entity has contravened a requirement.

314. Subsection (4) states that a confirmation decision must be given without delay and that it must include reasons for the decision.

315. Subsection (5) states that a confirmation decision may require the person to immediately comply with the requirement being contravened and/or remedy the consequences of the contravention. It may also specify a time period within which this must be done.

316. Subsection (6) states that the confirmation decision may require the person, within a specified period of time, to pay the penalty specified in the notification, or a lesser penalty that the enforcement authority considers appropriate in light of any representations received or steps taken to comply with the requirement. Daily penalties will begin to accrue in line with **clause 48(6)** and become payable under subsection (6). A penalty decision may only be appealed by judicial review heard in the High Court.

317. Subsections (7) and (8) require the recipient of a confirmation decision to comply with it and that that this duty to comply may be enforced through civil proceedings.

318. Subsections (9) and (10) allow the enforcement authority to require a person given a confirmation decision not to disclose the existence or the contents of the confirmation decision without the authority's permission if the Secretary of State considers that such disclosure would be contrary to the interests of national security.

Clause 51: Enforcement of penalty

319. **Clause 51** sets out how penalties may be enforced in England and Wales, Scotland and Northern Ireland.

320. Subsection (1) states that this clause applies for penalties imposed under **clause 50**.

321. Subsection (2) sets out how penalties imposed under **clause 50** may be recovered and/or enforced in England and Wales, Scotland and Northern Ireland.

322. Subsection (3) provides further details on how a penalty imposed under **clause 50** will be treated by the courts in England and Wales and Northern Ireland when recovery action is taken.

Clause 52: Enforcement of non-disclosure requirements

323. **Clause 52** sets out how breaches of non-disclosure requirements will be enforced, including the process for enforcement and the associated penalties.

324. Subsection (1) defines a "non-disclosure requirement" as a requirement imposed under **clause 43(11), 48(9),** or **50(9).**

325. Subsection (2) states that where a person is subject to a non-disclosure requirement, disclosure by an employee of that person or by a person engaged in the person's business will be regarded as a disclosure by the person, unless they can show that they took all reasonable steps to prevent disclosure.

326. Subsection (3) provides that **clauses 48 to 51** apply in relation to a contravention of a non-disclosure requirement as they apply in relation to a contravention of a relevant requirement with the modifications outlined in the following subsections.

327. Subsection (4) states that a notification of contravention under **clause 48** in relation to breach of a non-disclosure requirement must specify the steps that the Secretary of State thinks should be taken to bring the contravention to an end or limit the consequences of the contravention.

328. Subsection (5) provides that the maximum penalty for a contravention of a non-disclosure requirement is £10 million. In the case of a continuing contravention, the maximum daily penalty is £50,000 per day.

329. Subsection (6) states that a confirmation decision under **clause 50** may require the person to immediately end the contravention and/ or remedy the consequences of the contravention or specify a time period within which this must be done. The Secretary of State may issue a lesser penalty that the Secretary of State considers appropriate having regard to any steps taken to end the contravention or limit the consequences of the contravention.

Clause 53: Power to direct regulatory authorities

330. **Clause 53** grants the Secretary of State the power to issue a direction to a regulator where this is necessary and proportionate for national security.

331. Subsections (1) and (2) grant the Secretary of State the power to issue a direction to a regulator if the Secretary of State considers it to be necessary and proportionate in the interests of national security.

332. Subsection (3) establishes that a direction to a regulator may require it to provide information about how it has complied, or how it intends to comply, with the direction.

333. Subsection (4) lists the information that must be included in a direction. This includes 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, and 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.

334. Subsection (5) states that a regulator that receives a direction given under this section must comply with it.

335. Subsection (6) states that a direction under this section may not be given to a Minister of the Crown, a member of the Scottish Government or a junior Scottish minister, the Welsh Government, or a Northern Ireland Department.

Clause 54: Review, variation and revocation of directions

336. **Clause 54** establishes the requirement for the Secretary of State to review directions issued under **clauses 43** and **53**, and the process for varying or revoking them.

337. Subsection (1) specifies that this section applies to a direction given under **clauses 43** and **53.**

338. Subsection (2) requires the Secretary of State to review a direction from time to time. This subsection also allows the Secretary of State to vary or revoke a direction.

339. Subsection (3) says that a direction may only be varied if the Secretary of State considers this to be necessary and proportionate in the interests of national security.

340. Subsections (4) and (5) state that, if a direction is varied, the Secretary of State must notify the person to whom the direction was issued. Subsection (5) lists the information that must be included in the notice.

341. Subsection (6) requires the Secretary of State to provide notice to the person or persons subject to a direction if a direction is revoked. This notice must specify when the revocation comes into force.

342. Subsections (7) and (8) require the Secretary of State to consult a person before varying a direction to which the person is subject, unless to do so would be impracticable or contrary to national security. The Secretary of State may also consult any other person considered appropriate, such as the relevant regulator or lead government department.

343. Subsection (9) allows the Secretary of State to require a person consulted not to disclose the existence or the contents of the consultation, without the Secretary of State's permission. The Secretary of State may not impose this requirement unless the Secretary of State considers that disclosure would be contrary to the interests of national security (subsection (10)).

344. Subsection (11) states that the enforcement procedure and penalties for breaches of non-disclosure requirements in **clause 52** also apply to non-disclosure requirements in this section.

Clause 55: Laying before Parliament

345. **Clause 55** establishes the requirement for directions given under **clauses 43** and **53,** including variations under **clause 54**, to be laid before Parliament.

346. Subsection (1) requires the Secretary of State to lay directions given under **clause 43** and **clause 53** before Parliament (including variations under **clause 54**).

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

348. Subsection (3) allows the Secretary of State to exclude anything that, if published, would unreasonably prejudice the commercial interests of any person or would be contrary to the interests of national security, from what is laid before Parliament.

Clause 56: Information sharing

349. **Clause 56** sets out the conditions in which the Secretary of State or a regulator may disclose information for national security purposes.

350. Subsections (1) and (2) specify that the Secretary of State or a regulator may disclose information obtained under the powers in this Part of the Bill to a regulator, GCHQ, any other UK public authority or an overseas public authority (defined in subsection (6)).

351. Subsection (3) requires that a disclosure under this clause must be necessary for national security purposes and limited to information which is relevant and proportionate to the purpose of the disclosure.

352. Subsections (4) and (5) set out that disclosure of information under this clause does not breach any obligation of confidence owed by the disclosing person or any other restriction on the disclosure of information. However, this clause does not authorise disclosure if the disclosure would contravene the data protection legislation or is prohibited by Parts 1 to 7 or 9 of the Investigatory Powers Act 2016.

353. Subsection (6) defines "overseas public authority" as a person in any country or territory outside the UK which appears to the person proposing to disclose information to exercise certain functions of a public nature. Those functions are those which correspond to the functions of the Secretary of State under Part 4 or to the functions of a regulatory authority, or which relate to national security. "UK public authority" is defined as a person exercising functions of a public nature in the UK.

Example: Use of the Power

There has been a significant change in the geopolitical environment. After a period of heightened tension, Country X has invaded Country Y. The UK is an ally of Country Y. HMG understands that in order to disrupt an allied military response to the conflict, offensive cyber actions are likely to be taken by one or more countries involved (or drawn in). Given the increased offensive threat, systems in these sectors may need to be hardened. The type of action that might be necessary will vary between and within sectors but could include disconnecting remote access to operational technology, increased monitoring and logging on networks, or disabling functionality in networks.

In such a situation, the Secretary of State might consider using the Power of Direction to mandate that a NIS regulator updates their guidance to advise regulated entities to, during a time-bounded period, take action to put pre-arranged plans for hardening their cyber posture into practise or take certain actions to fulfil their duty to take 'appropriate and proportionate' security measures.

Clause 57: Means of giving directions and notices

354. Subsection (1) details the ways through which a direction or notice may be given to a person.

355. Subsection (2) defines "relevant individual".

356. Subsections (3) and (4) clarify what is meant by a person's proper address.

357. Subsection (5) defines that the person's email address is an email address published by the person as an address for contacting that person. If there is no such published address, the notice or direction can be sent to an email address that the person giving the direction or notice reasonably believes will bring the notice or direction to the attention of the receiving person.

358. Subsection (6) states that, unless otherwise proved, a direction or notice emailed to a person is deemed to have been given at 9am on the following working day. Subsection (7) clarifies that "working day" is any day other than the weekend or a bank holiday.

359. Subsection (8) states that, for the purposes of issuing a direction or notice, an "officer" of a body corporate refers to a director, manager, secretary or similar office holder in the body corporate.

Clause 58: Interpretation of Part 4

360. **Clause 58** defines a number of terms used in this Part of the Bill.

Part 5: General

Clause 59: Extent

361. **Clause 59** details the territorial extent of the provisions in the Bill as extending to England and Wales, Scotland and Northern Ireland.

Clause 60: Commencement

362. **Clause 60** provides for the commencement of the provisions in this Bill.

363. Subsection (1) sets out the provisions that will come into force on the day the Bill receives Royal Assent. This commences Part 1 of the Bill which sets out key definitions for the services in scope of NIS and regulators and enables Secretary of State to make regulations to bring more sectors into scope, appoint new regulators and update the NIS Regulations. It will also commence reporting requirements (**clause 40**) upon Royal Assent.

364. Subsection (2) sets out the provisions that will come into force two months after the day on which the Bill receives Royal Assent. They are provisions on the use and sharing of information under the NIS Regulations, Statement of Strategic Priorities etc., as well as consequential changes to the NIS National Strategy.

365. Subsection (3) sets out that the remaining provisions of the Bill will come into force on a day appointed in regulations by the Secretary of State. This includes measures to bring new services (data centres, RMSPs) into scope, measures to enable regulators to designate critical suppliers and new powers for Secretary of State to direct regulators and regulated entities.

366. Subsection (4) sets out that different days may be appointed for different purposes.

367. Subsections (5) and (6) provides that the only day which can be appointed for the coming into force of **clause 12** (critical suppliers) is the day on which the first set of regulations under **clause 29(1)** which amend the NIS Regulations by imposing requirements on persons which provide activity-critical suppliers comes into force. This restriction ensures that persons cannot be designated as critical suppliers before regulations under **clause 29** setting out the duties to which such persons, once

designated, will be subject have been made.

368. Subsection (7) enables the Secretary of State to make transitional or saving provision in connection to any provision of this Act.

369. Subsection (8) sets out that the power to make regulations includes the power to make different provision for different purposes.

370. Subsection (9) sets out that any power to make regulations under this section is exercisable by statutory instrument.

Clause 61: Short title

371. **Clause 61** provides the short title of the legislation as the Cyber Security and Resilience (Network and Information Systems) Act 2026.

Schedules

Schedule 1 – Enforcement, penalties and appeals

372. **Schedule 1** makes a series of amendments to the NIS Regulations for the purpose of updating the enforcement, appeals and penalties regime in conjunction with the changes made in the rest of this Bill.

Schedule 2 – Minor and consequential amendments etc

373. **Schedule 2** makes a series of detailed amendments to the NIS Regulations to integrate the new framework for the regulation of RMSPs. These amendments are made across all relevant regulations to systematically integrate RMSPs into the existing NIS Regulations and ensure parity with RDSPs in terms of oversight, enforcement, and accountability.

Financial implications of the Bill

374. The monetised costs and benefits of the Bill have been set out in the Bill's Impact Assessment.

Parliamentary approval for financial costs or for charges involved

375. The Bill requires a money resolution and a ways and means resolution.

376. A money resolution is required where a bill authorises new charges on the public revenue – broadly speaking, new public expenditure. In this case a money resolution is required because the Bill extends the regulatory functions of the Secretary of State and other public authorities by adding to the sectors and services which are regulated by them, and because it will lead to increased expenditure by publicly funded persons in complying with new requirements imposed under or by virtue of the Bill. The Bill also confers various functions on the Secretary of State that could result in additional

expenditure, including a power to make regulations under which further provision could be made which might lead to additional public expenditure.

377. A ways and means resolution is required where a bill authorises new charges on the people – broadly speaking, new taxation or other similar charges. As this Bill enables a regulator to impose charges in relation to their functions under the Bill that could be characterised as charges on the people (and also includes a power enabling regulations to make such provision), a ways and means resolution is required.

378. The ways and means resolution also contains a limb authorising payments into the Consolidated Fund, because the Bill amends the NIS Regulations which contain an express provision requiring payment of penalties into the Consolidated Fund.

Compatibility with the European Convention on Human Rights

374. The Secretary of State for Science, Innovation and Technology considers that the Cyber Security and Resilience (Network and Information Systems) Bill engages Articles 6, 7 and 8 and Article 1 Protocol 1 of the European Convention on Human Rights, but it is compatible with those articles. The Secretary of State for Science, Innovation and Technology considers that the powers to make delegated legislation under the Bill may, in the future, be exercised compatibly with the Convention rights.

375. The Secretary of State for Science, Innovation and Technology, Liz Kendall MP, has made the following statement under Section 19(1)(a) of the Human Rights Act 1998:

"In my view the provisions of the Cyber Security and Resilience (Network and Information Systems) Bill are compatible with the Convention rights."

Compatibility with the Environment Act 2021

376. The Secretary of State for Science, Innovation and Technology, Liz Kendall MP, is of the view that the Cyber Security and Resilience (Network and Information Systems) Bill as introduced into the House of Commons does not contain provisions which, if enacted, would affect environmental law for the purposes of Section 20 of the Environment Act 2021. Accordingly, no statement under that section has been made.

Compatibility with the European Union (Withdrawal) Act 2018

377. The Secretary of State for Science, Innovation and Technology, Liz Kendall MP, is of the opinion that the Cyber Security and Resilience (Network and Information Systems) Bill does not contain provisions which, if enacted, would affect trade between Northern Ireland and the rest of the UK. Accordingly, no statement under Section 13C of the European Union (Withdrawal) Act 2018 has been made.

Subject matter and legislative competence of devolved legislatures

378. The main subject matter of this Bill is cyber security regulation, which is an area of reserved legislative competence.

379. The provisions of the Bill are not devolved to any of the three Devolved Governments. However, they alter the executive competence of regulators responsible for NIS sectors within each Scotland, Wales, and Northern Ireland through amendments to the NIS Regulations. A Legislative Consent Motion has been requested from the Welsh and Scottish Governments and the Northern Ireland Executive for these areas.

Annex A: Territorial extent

380. **Clause 59** sets out that the Bill extends to the whole of the UK.

381. **Part 2** of the Bill amends the NIS Regulations 2018 and has the same application as those Regulations. The NIS Regulations apply to the UK, including its internal waters, the territorial sea adjacent to the UK, and the sea (including the seabed and subsoil) in any area designated under section 1(7) of the Continental Shelf Act 1964 (regulation 1(6) of the NIS Regulations).

382. In addition, the Bill makes specific provision on application for regulations made under **clause 24** or **Part 3** of the Bill and the directions to regulated entities under **clause 43**, which tracks the application of the NIS Regulations themselves (**clause 41(e)** and **clause 43(3)(h)**). The application of the rest of the Bill is to the UK.

383. The UK Parliament does not normally legislate with regard to matters that are within the legislative competence of the Scottish Parliament, the Senedd Cymru or the Northern Ireland Assembly without the consent of the legislature concerned.

384. It is also the practice of the UK Government to seek the consent of the devolved legislatures for provisions which would alter the competence of those legislatures or the devolved administrations in Scotland, Wales and Northern Ireland.

385. The provisional assessment of the UK Government concludes that the provisions within the Bill are reserved under the telecommunications and national security reservations for Scotland and Wales and the telecommunications reservation and national security exception for Northern Ireland.

386. Some of the provisions of the Bill alter the executive functions of regulators, some of whom are Devolved Governments. The UK Government has engaged with each of the Devolved Governments to formally agree the provisions where the consent of the devolved legislatures should be sought.

Annex B: Related documents

387. The following documents are relevant to the Bill and can be read at the stated locations:

a. Cyber security and resilience policy statement

b. King's Speech 2024: background briefing notes

c. Government response to the call for views on proposals to improve the UK's cyber resilience

d. Proposal for legislation to improve the UK's cyber resilience and consultation

e. Cyber Security and Resilience (Network and Information Systems) Bill Impact Assessment

f. Cyber Security and Resilience (Network and Information Systems) Bill Delegated Powers Memorandum

CYBER SECURITY AND RESILIENCE (NETWORK AND INFORMATION SYSTEMS) BILL

EXPLANATORY NOTES

These Explanatory Notes relate to the Cyber Security and Resilience (Network and Information Systems) Bill as introduced in the House of Commons on 12 November 2025 (Bill 329).

Ordered by the House of Commons to be printed, 12 November 2025

PUBLISHED BY AUTHORITY OF THE HOUSE OF COMMONS