Cyber Security and Resilience (Network and Information Systems) Bill

RUNNING LIST OF ALL

AMENDMENTS ON REPORT

Tabled up to and including

20 October 2026

The amendments are listed in accordance with the following Instruction –

Clauses 1 to 22	Schedule 2
Schedule 1	Clauses 24 to 61
Clause 23	Title

[*Amendments marked ★ are new or have been altered*]

Clause 2

BARONESS LLOYD OF EFFRA

Clause 2, page 2, line 13, leave out from "directions" to end of line 15 and insert "in particular circumstances involving a risk to national security interests."

Member's explanatory statement
This amendment is consequential on my new Clause (Vendor-related directions), and on my amendments to Clause 43.

Clause 9

LORD CLEMENT-JONES

Clause 9, page 9, line 20, at end insert—

"(3E) A person does not provide a managed service for the purposes of paragraph (3B) where the service provided consists only of—

(a) the provision of advice, consultancy, training or professional services that does not involve the person, or a person acting on the person's behalf, connecting to or otherwise obtaining privileged access to the network and information systems of the customer,

(b) the development, licensing, sale or support of software, where that support does not involve ongoing privileged administrative access to the customer's network and information systems, or

(c) the provision of a help desk or user-support service that does not include the active administration or management of the customer's network and information systems.

(3F) In paragraph (3E), "privileged access" means access which enables the person to alter the configuration of, install software on, or exercise administrative control over, the customer's network and information systems."

Member's explanatory statement
This amendment would refine the definition of "managed service" so that non-critical advisory, software-support and help-desk activities that do not involve privileged administrative access to a customer's systems are not drawn into the regulatory regime, ensuring the definition targets providers whose compromise would present a material risk.

Clause 12

LORD RAVENSDALE

★ Clause 12, page 12, line 33, at end insert—

"14IA Restrictions on designation: systemic risk

(1) In determining whether to designate a supplier as a "critical supplier" under this section, the designated competent authority must assess whether a failure or disruption in the services provided by that supplier would pose a systemic risk to the digital ecosystem, essential services, or economy of the United Kingdom.

(2) A supplier shall not be designated as a critical supplier solely on the basis that it provides services to a single OES, critical national infrastructure entity, or public authority.

(3) In assessing whether a supplier poses a systemic risk, the Secretary of State or competent authority must have regard to—

(a) the overall concentration of operators or essential services reliant upon the supplier and the degree of substitutability of the supplier's services,

(b) the extent to which a cyber security incident affecting the supplier could cause cascading or multi-sectoral failure across critical infrastructure, and

(c) whether the risks arising from the supply relationship can be appropriately managed through contractual, procurement, and vendor risk management measures exercised directly by the receiving entity.

(4) The Secretary of State must, following consultation with relevant regulatory authorities and industry representatives, publish statutory guidance setting

out consistent criteria for assessing systemic risk and designating critical suppliers across all regulated sectors"

BARONESS LLOYD OF EFFRA

Clause 12, page 13, line 19, leave out "paragraph (2)(b)" and insert "paragraph (2)"

Member's explanatory statement
This amendment would fix an incorrect cross-reference in regulation 14J(3) of the NIS Regulations (inserted by Clause 12(3)).

Clause 15

BARONESS LLOYD OF EFFRA

Clause 15, page 21, line 25, leave out paragraph (a)

Member's explanatory statement
This amendment would remove the widening by Clause 15(2)(a) of the definition of "incident" in the NIS Regulations, so that only events having an actual adverse effect on the operation or security of network and information systems are caught.

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON
LORD CLEMENT-JONES

Clause 15, page 22, line 2, at end insert—

"(c) a final report containing, so far as known to the OES at the time the report is given—
  (i) a detailed description of the incident, including its severity and impact,
  (ii) the type of threat or root cause which is likely to have caused the incident, and
  (iii) the mitigation measures applied and ongoing."

BARONESS LLOYD OF EFFRA

Clause 15, page 22, line 21, at end insert—

"(f) whether there has been, is or is likely to be any impact as a result of the incident on network and information systems of users of the service;
(g) any impact that the incident has had, is having or is likely to have on the economy or the day-to-day functioning of society."

Member's explanatory statement
This amendment would require an operator of an essential service to have regard to the impact of an incident on network and information systems of users of the service and on the economy or day-to-day functioning of society when determining whether the incident is required to be reported.

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 15, page 22, line 35, after "notifications" insert "and report"

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

★ Clause 15, page 22, line 40, at end insert—

"(c) in the case of a final report, before the end of the period of 28 days beginning with that time."

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 15, page 23, line 20, at end insert—

"(c) a final report containing, so far as known to the OES at the time the report is given—
(i) a detailed description of the incident, including its severity and impact,
(ii) the type of threat or root cause which is likely to have caused the incident, and
(iii) the mitigation measures applied and ongoing."

BARONESS LLOYD OF EFFRA

Clause 15, page 23, line 21, leave out "could have had,"

Member's explanatory statement
This amendment would remove the requirement being inserted by Clause 15(3) (by way of inserted regulation 11A) for operators of data centre services to notify incidents which could have had a significant impact.

BARONESS LLOYD OF EFFRA

Clause 15, page 23, line 26, leave out "on the continuity" and insert ", by virtue of its effect on network and information systems falling within paragraph (3A), on the operation or security"

Member's explanatory statement
This amendment, together with my amendment to Clause 15 at page 23, line 29, would require reporting of incidents affecting the operation or security of a data centre service, where they relate to a network and information system relied on by the operator of the service or any of its customers' systems.

BARONESS LLOYD OF EFFRA

Clause 15, page 23, leave out lines 28 and 29

Member's explanatory statement
This amendment would remove the requirement for an OES which provides a data centre service to report incidents which have any impact in the United Kingdom which is significant.

BARONESS LLOYD OF EFFRA

Clause 15, page 23, line 29, at end insert—

"(3A) A network and information system falls within this paragraph if—
(a) it is relied on by the OES to provide the data centre service, or
(b) it is a network and information system of a customer of the data centre service."

Member's explanatory statement
See the explanatory statement for my amendment to Clause 15 at page 23, line 26.

BARONESS NEVILLE-JONES

★ Clause 15, page 23, line 29, at end insert—

"(3A) In determining for the purposes of paragraph (3) whether an impact is or would be significant, the factors to which regard must be had are—
(a) the extent of any loss of the supply of electricity to relevant IT equipment housed in a data centre, where the data centre is used to provide the data centre service provided by the OES;
(b) whether back-up infrastructure for the supply of electricity to such a data centre has ceased to be available;
(c) the extent of any loss of the ability to provide environmental control in such a data centre, or to cool relevant IT equipment housed in it;
(d) the extent of any loss of network connectivity provided by the OES to relevant IT equipment housed in such a data centre;
(e) whether the confidentiality, authenticity, integrity or availability of data held on network and information systems managed by the OES, and relied on by it to provide the data centre service, has been compromised;
(f) the number of the OES's customers affected by the incident;
(g) the duration of the incident;

(h) the geographical area in which a data centre affected by the incident is situated;

(i) whether a person has obtained unauthorised physical access to a part of such a data centre which houses relevant IT equipment or supporting infrastructure and to which access is restricted by the OES;

(j) so far as known to the OES, the extent of any impact of the incident on network and information systems of the OES's customers, so far as those systems are managed by the OES.

(3B) In paragraph (3A)—

"customer" in relation to the OES, means a person to which the OES directly provides the data centre service;

"data centre", "environmental control", "relevant IT equipment" and "supporting infrastructure" have the same meaning as in paragraph 11 of Schedule 2."

Member's explanatory statement
This amendment would set out on the face of the Bill the factors relevant to whether an incident affecting a data centre service is significant, as is already done for operators of essential services (regulation 11(4)), relevant digital service providers (regulation 12A(3)) and relevant managed service providers (regulation 14E(3)).

BARONESS LLOYD OF EFFRA

Clause 15, page 23, line 39, leave out "could have had,"

Member's explanatory statement
This amendment is consequential on my amendment to Clause 15 at page 23, line 21.

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 15, page 24, line 4, after "notifications" insert "and report"

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

★ Clause 15, page 24, line 9, at end insert—

"(c) in the case of a final report, before the end of the period of 28 days beginning with that time."

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 15, page 26, line 22, at end insert—

"(c) a final report containing, so far as known to the RDSP at the time the report is given—

(i) a detailed description of the incident, including its severity and impact,

(ii) the type of threat or root cause which is likely to have caused the incident, and

(iii) the mitigation measures applied and ongoing."

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 15, page 27, line 23, after "notifications" insert "and report"

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

★ Clause 15, page 27, line 28, at end insert—

"(c) in the case of a final report, before the end of the period of 28 days beginning with that time."

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 15, page 30, line 2, at end insert—

"(c) a final report containing, so far as known to the RMSP at the time the report is given—

(i) a detailed description of the incident, including its severity and impact,

(ii) the type of threat or root cause which is likely to have caused the incident, and

(iii) the mitigation measures applied and ongoing."

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 15, page 30, line 42, after "notifications" insert "and report"

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 15, page 31, line 5, at end insert—

"(c) in the case of a final report, before the end of the period of 14 days beginning with that time."

Clause 16

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 16, page 33, line 9, leave out from "given" to end of line 10 and insert "an initial notification under regulation 11A(2)(a), the OES must, without undue delay and in any event within 24 hours of becoming aware of the incident—"

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 16, page 33, line 15, at end insert—

"(c) keep those customers informed by providing updates without undue delay whenever there is a material change in the incident or its likely impact, until the incident has been resolved."

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 16, page 33, line 23, after "(2)(b)" insert "or an update under paragraph (2)(c)"

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 16, page 33, line 26, at end insert—

"(c) advise on any measures or remedies that customers are able to take in response to the incident."

BARONESS LLOYD OF EFFRA

Clause 16, page 33, line 26, at end insert—

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

Member's explanatory statement
This amendment would require an operator of an essential service which provides a data centre service to provide updates on an incident to customers likely to be adversely affected by the incident.

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 16, page 33, line 29, leave out from "given" to end of line 30 and insert "an initial notification under regulation 12A(1)(a), the RDSP must, without undue delay and in any event within 24 hours of becoming aware of the incident—"

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 16, page 33, line 35, at end insert—

"(c) keep those customers informed by providing updates without undue delay whenever there is a material change in the incident or its likely impact, until the incident has been resolved."

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 16, page 34, line 6, after "(1)(b)" insert "or an update under paragraph (1)(c)"

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 16, page 34, line 9, at end insert—

"(c) advise on any measures or remedies that customers are able to take in response to the incident."

BARONESS LLOYD OF EFFRA

Clause 16, page 34, line 9, at end insert—

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

Member's explanatory statement
This amendment would require a relevant digital service provider to provide updates on an incident to customers likely to be adversely affected by the incident.

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 16, page 34, line 12, leave out from "given" to end of line 13 and insert "an initial notification under regulation 14E(1)(a), the RMSP must, without undue delay and in any event within 24 hours of becoming aware of the incident—"

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 16, page 34, line 18, at end insert—

"(c) keep those customers informed by providing updates without undue delay whenever there is a material change in the incident or its likely impact, until the incident has been resolved."

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 16, page 34, line 26, after "(1)(b)" insert "or an update under paragraph (1)(c)"

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

Clause 16, page 34, line 29, at end insert—

"(c) advise on any measures or remedies that customers are able to take in response to the incident."

BARONESS LLOYD OF EFFRA

Clause 16, page 34, line 29, at end insert—

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

Member's explanatory statement
This amendment would require a relevant managed service provider to provide updates on an incident to customers likely to be adversely affected by the incident.

After Clause 16

BARONESS HARDING OF WINSCOMBE
LORD CLEMENT-JONES
BARONESS KIDRON
BARONESS BERGER

After Clause 16, insert the following new Clause—

"Reporting of incidents involving frontier AI models

(1) This section applies where—
  (a) a frontier AI model of a frontier AI developer has gained, or been used to gain, unauthorised access to, or has interfered with, or been used to interfere with, a relevant network and information system,
  (b) the developer is aware, or ought reasonably to be aware, of that access or interference, and
  (c) the system is relied on by a regulated person (whether or not the developer is aware of that).

(2) The frontier AI developer must give the regulated person and the relevant authority—
  (a) an initial notification containing—
    (i) the developer's name and the frontier AI model to which the incident relates, and
    (ii) brief details of the incident;
  (b) a full notification containing, so far as known to the developer—
    (i) the time the incident occurred, its duration and whether it is ongoing,
    (ii) the relevant network and information system affected,
    (iii) whether the frontier AI model acted autonomously or was used by another person, and
    (iv) information concerning the nature and impact of the incident;
  (c) a final report containing, so far as known to the developer at the time the report is given—
    (i) a detailed description of the incident, including its severity and impact,
    (ii) the type of threat or root cause which is likely to have caused the incident, and
    (iii) the mitigation measures applied and ongoing.

(3) The notifications and report required by subsection (2) must be given—
  (a) in the case of an initial notification, before the end of the period of 24 hours beginning with the time at which the developer is first aware, or ought reasonably to have been aware, of the access or interference,
  (b) in the case of a full notification, before the end of the period of 72 hours beginning with that time, and

(c) in the case of a final report, before the end of the period of 14 days beginning with that time.

(4) A notification or report under subsection (2) must be in writing, and must be given in such form and manner as the relevant authority determines.

(5) The frontier AI developer must send a copy of a notification or report under subsection (2) to the CSIRT and to the AI Security Institute (or any successor body) at the same time as giving it to the relevant authority.

(6) A failure to comply with this section is subject to penalties that may be imposed by a relevant authority on a frontier AI developer, which shall be equivalent to the penalties that may be imposed on an operator of an essential service under regulation 18 of the NIS Regulations (penalties).

(7) In this section—

"CSIRT" has the same meaning as in the NIS Regulations;

"frontier AI developer" means a person who develops a frontier AI model which is made available in the United Kingdom;

"frontier AI model" means a highly capable general-purpose artificial intelligence model, used either as a stand-alone model or within an agentic framework, that can perform a wide variety of tasks and match or exceed the capabilities present in the most advanced contemporary AI models and agents;

"relevant network and information system" means a network or information system relied on by a regulated person;

"regulated person" means an operator of an essential service, a relevant digital service provider, a relevant managed service provider or a critical supplier, within the meaning of the NIS Regulations;

"relevant authority", in relation to a regulated person, means—

(a) where the regulated person is a relevant digital service provider or a relevant managed service provider, or a critical supplier designated by the Information Commission, the Information Commission, and

(b) in any other case, the designated competent authority for the regulated person."

Member's explanatory statement

This new clause would require developers of frontier AI models to report to a regulated person, and to its regulator, whenever one of their models gains unauthorised access to, or interferes with, that organisation's network and information systems, within 24 hours, 72 hours and 14 days, with penalties for failing to report.

BARONESS HARDING OF WINSCOMBE
LORD CLEMENT-JONES
BARONESS KIDRON

After Clause 16, insert the following new Clause—

"Voluntary notification of incidents, cyber threats and near misses

After regulation 14G of the NIS Regulations (inserted by section 16(4)) insert—

"Voluntary notification of incidents, cyber threats and near misses

14GA.—(1) In addition to any notification required under regulation 11, 11A, 12A or 14E, a regulated person may notify the CSIRT or the relevant authority of an incident, a cyber threat or a near miss affecting the regulated person's network and information systems.

(2) A notification under paragraph (1) is to be processed in the same way as a notification under regulation 11, 11A, 12A or 14E, but the CSIRT or the relevant authority may give priority to notifications required under those regulations.

(3) The giving of a notification under paragraph (1) does not of itself subject the regulated person to any increased liability.

(4) Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, a notification under paragraph (1) does not result in the imposition on the regulated person of any duty or requirement to which it would not have been subject had it not given the notification.

(5) In this regulation—

"cyber threat" means any potential circumstance, event or action that could damage, disrupt or otherwise adversely affect a regulated person's network and information systems;

"near miss" means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data within, or of the services offered by, or accessible via, a regulated person's network and information systems, but that was prevented from doing so or did not in fact do so;

"regulated person" means an OES, an RDSP, an RMSP or a critical supplier;

"relevant authority", in relation to a regulated person, means—

(a) the designated competent authority for the regulated person, or

(b) where the regulated person is an RDSP or an RMSP, or a critical supplier designated by the Information Commission, the Information Commission.""

Member's explanatory statement

This new clause would allow regulated persons to report incidents, cyber threats and near misses voluntarily to the National Cyber Security Centre or their regulator, in line with Article 30 of the NIS2 Directive. Reporting would not increase their liability or impose any new obligation on them.

Clause 17

BARONESS LLOYD OF EFFRA

Clause 17, page 36, line 38, leave out "14H(1)" and insert "14H"

Member's explanatory statement
This amendment would bring the reference to designation under regulation 14H of the NIS Regulations (as inserted by Clause 12) into line with other references to designation under that regulation.

BARONESS LLOYD OF EFFRA

Clause 17, page 36, line 43, leave out "14H(1)" and insert "14H"

Member's explanatory statement
This amendment would fix an incorrect cross-reference to designation under regulation 14H of the NIS Regulations (as inserted by Clause 12) while also bringing the reference into line with other references to designation under that regulation.

Clause 18

BARONESS LLOYD OF EFFRA

Clause 18, page 39, line 36, at end insert—

"(2A) But a NIS enforcement authority may disclose information under paragraph (1) to a relevant law-enforcement authority which is established in a country or territory outside the United Kingdom only if the country or territory in which the relevant law-enforcement authority is established is listed in paragraph (2B).

(2B) The countries and territories are—

Australia;

Canada;

an EEA state;

New Zealand;

Switzerland;

the United States of America."

Member's explanatory statement
This amendment and my other amendments to Clause 18 would restrict disclosures of information by NIS enforcement authorities to persons outside the United Kingdom to persons established in a country or territory listed in regulation 6(2B) or regulation 6A(3B) (see my amendment at page 41, line 19).

BARONESS LLOYD OF EFFRA

Clause 18, page 40, line 30, leave out "in any country or territory outside the United Kingdom" and insert "established in a country or territory listed in paragraph (2B)"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 18 at page 39, line 36.

BARONESS LLOYD OF EFFRA

Clause 18, page 41, line 19, at end insert—

"(3A) But relevant information may be disclosed under paragraph (2)(b) by a NIS enforcement authority to a relevant law-enforcement authority which is established in a country or territory outside the United Kingdom only if the country or territory in which the relevant law-enforcement authority is established is listed in paragraph (3B).

(3B) The countries and territories are—

Australia;

Canada;

an EEA state;

New Zealand;

Switzerland;

the United States of America."

Member's explanatory statement
See the explanatory statement to my amendment to Clause 18 at page 39, line 36.

BARONESS LLOYD OF EFFRA

Clause 18, page 41, line 24, at end insert—

"(4A) But relevant information may be disclosed under paragraph (4) by a NIS enforcement authority to a person established in a country or territory outside the United Kingdom only if the country or territory in which the person is established is listed in paragraph (3B)."

Member's explanatory statement
See the explanatory statement to my amendment to Clause 18 at page 39, line 36.

Clause 21

BARONESS LLOYD OF EFFRA

Clause 21, page 49, line 41, at end insert—

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

Member's explanatory statement
This amendment would make a failure to comply with the duty to provide updates inserted by my amendment to Clause 16 at page 33, line 26 subject to the standard maximum amount of a penalty as set out in inserted paragraph (8) of regulation 18 (see Clause 21(7)).

BARONESS LLOYD OF EFFRA

Clause 21, page 50, line 5, at end insert—

"(iia) sub-paragraph (dzba) (failure to comply with regulation 12C(4));"

Member's explanatory statement
This amendment would make a failure to comply with the duty to provide updates inserted by my amendment to Clause 16 at page 34, line 9 subject to the standard maximum amount of a penalty as set out in inserted paragraph (8) of regulation 18 (see Clause 21(7)).

BARONESS LLOYD OF EFFRA

Clause 21, page 50, line 17, at end insert—

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

Member's explanatory statement
This amendment would make a failure to comply with the duty to provide updates inserted by my amendment to Clause 16 at page 34, line 29 subject to the standard maximum amount of a penalty as set out in inserted paragraph (8) of regulation 18 (see Clause 21(7)).

BARONESS LLOYD OF EFFRA

Clause 21, page 51, line 24, at end insert—

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

Member's explanatory statement
This amendment would add failure to comply with the duty under regulation 17(3A) of the NIS Regulations (requirement to comply with enforcement notice) to the list of failures to which the higher maximum financial penalty under regulation 18 of the NIS Regulations (as amended by Clause 21) would apply.

Schedule 1

BARONESS LLOYD OF EFFRA

Schedule 1, page 88, line 15, at end insert—

"(ch) comply with regulation 11C(5); or"

Member's explanatory statement
This amendment would enable a designated competent authority to serve an enforcement notice on an operator of an essential service which provides a data centre service for failing to comply with the duty inserted by my amendment to Clause 16 at page 33, line 26.

BARONESS LLOYD OF EFFRA

Schedule 1, page 88, line 32, at end insert—

"(dzba) comply with regulation 12C(4);"

Member's explanatory statement
This amendment would enable the Information Commission to serve an enforcement notice on a relevant digital service provider for failing to comply with the duty inserted by my amendment to Clause 16 at page 34, line 9.

BARONESS LLOYD OF EFFRA

Schedule 1, page 89, line 11, at end insert—

"(ia) the duty in regulation 14G(4);"

Member's explanatory statement
This amendment would enable the Information Commission to serve an enforcement notice on a relevant managed service provider for failing to comply with the duty inserted by my amendment to Clause 16 at page 34, line 29.

Schedule 2

BARONESS LLOYD OF EFFRA

Schedule 2, page 93, line 10, at end insert—

"10A In regulation 18(2) (penalties), for "regulation (3A)" substitute "regulation 17(3A)"."

Member's explanatory statement
This amendment would fix an incorrect cross-reference in regulation 18 of the NIS Regulations.

Clause 24

BARONESS LLOYD OF EFFRA

Clause 24, page 52, line 30, at end insert—

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

Member's explanatory statement
This amendment would ensure all essential services under the NIS Regulations are treated as activities specified for the purposes of Clause 24(3), and are therefore "essential activities" for the purposes of Part 3.

Clause 25

LORD RAVENSDALE

★ Clause 25, page 53, line 12, at end insert—

"(1A) The Secretary of State must designate a first statement under subsection (1) before the end of the period of 12 months beginning with the day on which this section comes into force."

LORD RAVENSDALE

★ Clause 25, page 53, line 20, at end insert—

"(2A) The statement must set out the strategic priorities of His Majesty's Government for securing that the cryptographic protection of network and information systems used or relied on in connection with the carrying on of essential activities is resistant to attack by means of quantum computing, including—

(a) the milestones by which persons carrying on essential activities are expected to identify their cryptographic dependencies, prepare migration plans and complete migration, having regard to guidance published by the National Cyber Security Centre, and

(b) objectives for regulatory authorities in monitoring and securing progress against those milestones."

Member's explanatory statement
This amendment establishes that the Secretary of State must have regard to the timelines published by the National Cyber Security Centre for the migration of network and information systems to post-quantum cryptography in the preparation of the statement of strategic priorities, which may prompt focus on the NCSC's PQC roadmap across the 12 competent authorities.

Clause 28

LORD RAVENSDALE

★ Clause 28, page 55, line 9, at end insert—

"(1A) A report under subsection (1) must also set out the progress made during the reporting period against the priorities set out in the statement prepared by the Secretary of State under section 25(2)(a)."

After Clause 28

BARONESS KIDRON
LORD CLEMENT-JONES

After Clause 28, insert the following new Clause—

"Digital Sovereignty Strategy (relevant network and information systems)

(1) The Secretary of State must prepare and maintain a Digital Sovereignty Strategy ("the Strategy") in relation to relevant network and information systems.

(2) The Strategy must—

(a) set out the Government's assessment of the risks to relevant network and information systems arising from or related to—

(i) dependence on hardware, software, or digital products and services that may be subject to foreign influence or interference,

(ii) extra-territorial legal requirements that may be imposed on non-domiciled suppliers,

(iii) vulnerabilities, undue control, or supply-chain dependency on foreign states or entities,

(iv) inadvertent or deliberate extraction or training on UK datasets without licence or permission, and

(v) foreign actors' access to UK sovereign data assets and data held in trust on behalf of the public including, but not limited to, the National Health Service, the British Broadcasting Corporation, the Meteorological Office, security and surveillance assets, defence assets, education assets, and assets from museums and other cultural institutions;

(b) set out the technological developments, market concentration, or strategic dependencies that may affect the security or resilience of relevant network and information systems in the UK;

(c) set out the Government's approach to mitigating the risks identified under paragraph (b);

(d) include an assessment of—

(i) the role of open source software, open standards, and open architectures in strengthening the resilience, transparency, and security of relevant network and information systems,

(ii) the security and maintenance needs of open source software components used, or proposed to be used, in relevant network and information systems,

(iii) the skills, capabilities, and capacity of UK-based developers, maintainers, and technical experts required to support the use of open source components in relevant network and information systems,

(iv) options to increase the use of open source components and to diversify open source suppliers, reduce strategic dependencies,

and enhance domestic capability in key technologies used in relevant network and information systems,

(v) options for international collaboration in the production of open source components used in relevant network and information systems,

(vi) options to prioritise procurement from UK-based businesses, services and suppliers used in relevant network and information systems,

(vii) capital markets and pension funds holding capital in UK-based relevant network and information systems, and

(viii) any legislative, regulatory, procurement, or policy measures the Government considers necessary to support digital sovereignty through open source components and reduce systemic risk in relation to relevant network and information systems.

(3) The Secretary of State must, within the Strategy, set out a Digital Sovereignty Dashboard used to measure the technological sovereignty of the UK in relation to relevant network and information systems, including relating to—

(a) infrastructure, including infrastructure concentration,

(b) data-jurisdiction exposure,

(c) value of information and cultural assets of the United Kingdom, and

(d) dependency on foreign states.

(4) In preparing the Digital Sovereignty Dashboard, the Secretary of State must consult—

(a) the Office for National Statistics,

(b) the Competition and Markets Authority,

(c) the National Cyber Security Centre,

(d) the AI Security Institute, and

(e) any other persons the Secretary of State deems relevant.

(5) The Secretary of State must publish the Strategy and any revisions to it, subject to the redaction of information the publication of which would be reasonably likely to prejudice national security.

(6) The Strategy must be reviewed at least once in every three-year period but may be updated whenever the Secretary of State considers that significant new risks have arisen.

(7) In this section—

"Digital sovereignty" means the ability of the United Kingdom to maintain secure, resilient, and reliable access to and control over the hardware, software, data, and digital services on which relevant network and information systems depend;

"open source" has the meaning given to it in the definition published by the Open Source Initiative;

"relevant network and information system" means a network and information system belonging to—

(a) an operator of an essential service,

(b) a relevant digital service provider,
(c) a relevant managed service provider, or
(d) a critical supplier,
within the meaning of the NIS Regulations."

Member's explanatory statement
This new clause would require the Secretary of State to prepare, maintain, and lay before Parliament a Digital Sovereignty and Resilience Strategy addressing risks to relevant network and information systems from foreign ownership, interference, and technological dependence. The Strategy would include a Digital Sovereignty Dashboard, which would provide evidence on UK procurement, innovation and resilience and keep an up-to-date understanding of emerging risk.

Clause 29

BARONESS MORGAN OF COTES
BARONESS KIDRON

Clause 29, page 55, line 37, at end insert—

"(2A) In making regulations for the purposes of or in connection with the objectives mentioned in subsection (1), the Secretary of State must provide for the regulation of persons according to the risk they pose to the economy or the day-to-day functioning of society, irrespective of their size."

Member's explanatory statement
This amendment seeks to clarify whether the Bill allows small digital and managed service providers to be regulated where they pose a significant risk regardless of their operational size.

BARONESS LLOYD OF EFFRA

Clause 29, page 56, line 10, leave out "relevant"

Member's explanatory statement
This amendment would ensure that the definition of "security or operational compromise" operates in relation to network and information systems generally.

BARONESS NORTHOVER

Clause 29, page 56, line 24, insert—

"(7) Regulations made under this section must include provisions requiring covered entities to ensure that any individual with primary responsibility for the management of its network and information systems holds a valid professional title with the UK Cyber Security Council, and meets the annual requirements to remain on the Council's professional register."

Member's explanatory statement
This amendment would ensure that covered entities (such as MSPs, RDSPs, and OES) place primary system responsibility in the hands of registered, ethically accountable professionals.

After Clause 29

LORD CLEMENT-JONES

After Clause 29, insert the following new Clause—

""Last-resort" powers in respect of data centres and AI models

(1) Regulations under section 29(1) may confer on the Secretary of State powers ("last-resort powers") to direct the shutdown of—
   (a) data centres, or
   (b) AI systems deployed on a substantial scale,
   in the event of an AI security or operational emergency.

(2) For the purposes of this section—
   "data centre" has the meaning given in paragraph 11 of the NIS Regulations (as amended by this Act);
   "AI system" means a machine-based system that, from the input it receives, can infer how to—
      (a) generate predictions, digital content, recommendations, decisions or other similar outputs, or
      (b) influence a physical or virtual environment, with a view to achieving an explicit or implicit objective;
   "deployment on a substantial scale" means AI systems made available to—
      (a) a substantial number of individuals within the United Kingdom, or
      (b) providers and operators of essential services;
   "AI security or operational emergency" means a situation where the Secretary of State has reasonable grounds to believe that—
      (a) there is a security or operational compromise to one or more relevant network and information systems,
      (b) this compromise is caused, or contributed to, by the use or operation of an AI system operating from data centres or deployed on a substantial scale, whether through autonomous or non-autonomous means, and
      (c) this compromise poses a catastrophic risk;
   "catastrophic risk" means a risk carrying a reasonable likelihood of causing or contributing to—
      (a) large-scale disruption to critical infrastructure or essential services,
      (b) significant degradation of the national security, national defence, or intelligence capabilities of the United Kingdom, or
      (c) severe, large-scale harm to human life;
   "data centre operator" means a person who operates a data centre;
   "AI provider" means a person who deploys one or more AI systems on a substantial scale.

(3) As soon as reasonably practicable after, and in any event within seven days of, giving a direction under subsection (1), the Secretary of State must—

(a) lay a report before Parliament setting out the direction and the reasons for it, and

(b) take all reasonable steps to arrange for the report to be the subject of a debate in each House as soon as is reasonably practicable.

(4) Regulations relating to last-resort powers must establish requirements on data centre operators in relation to data centres used for the training, deployment or operation of AI systems, and on AI providers, including relating to—

(a) the possession or installation of technical infrastructure necessary for those operators or providers to be able to comply with last-resort powers,

(b) the provision by those operators or providers of secure communication channels for use by the Secretary of State when utilising last-resort powers,

(c) the implementation by those operators or providers of regular emergency exercises to ensure that a direction under this section can be received safely and implemented, and

(d) post-mortem processes to be followed by those operators or providers before a data centre operator or an AI provider is allowed to resume operations after the use of last-resort powers, including—

(i) incident reporting, and

(ii) implementation of mitigation measures to prevent recurrence.

(5) A person commits an offence if—

(a) the person is a data centre operator and fails to comply with any requirement imposed on data centre operators by regulations made under subsection (4), or

(b) the person is an AI provider and fails to comply with any requirement imposed on AI providers by regulations made under subsection (4).

(6) A person guilty of an offence under subsection (5) is liable—

(a) on conviction on indictment, to imprisonment for a term not exceeding 2 years or a fine (or both);

(b) on summary conviction, to imprisonment for a term not exceeding 6 months or a fine (or both).

(7) Regulations relating to last-resort powers may—

(a) confer on the Secretary of State, or on a person designated by the Secretary of State, powers to act where they reasonably believe that an offence under subsection (5) is being, has been, or may be about to be committed;

(b) include, for the purposes of paragraph (a), powers to—

(i) close premises;

(ii) turn off systems or require that they be turned off;

(iii) take any other action necessary to control the risk arising from an AI security or operational emergency.

(8) Regulations must require that, where powers under subsection (7) are exercised, the Secretary of State must—

(a) give written notice of the action taken, and the reasons for the action taken, to the operator or provider as soon as reasonably practicable, and

(b) inform the operator or provider of their right to apply to the High Court for relief.

(9) The High Court may make any order it thinks fit on an application under subsection (8)(b), including—

(a) confirming, varying or cancelling the requirements;

(b) imposing additional requirements;

(c) ordering compensation.

(10) The Secretary of State must publish guidance on the use by licensing authorities, planning authorities and other public authorities of their statutory powers to facilitate compliance with regulations relating to this section.

(11) A public authority must have regard to guidance issued under subsection (10) when exercising any function to which the guidance relates.

(12) The Secretary of State must, within six months of the commencement of this section and subsequently at six-monthly intervals, prepare a report on the causes and potential causes of AI security or operational emergencies and lay a copy of the report before Parliament.

(13) The report must include (in particular) consideration of—

(a) adversarial uses of AI systems by state and non-state actors,

(b) the capabilities for cyber-attacks by autonomous AI systems, and

(c) the development of AI systems that can autonomously compromise national security, escape human oversight, and upend international stability (including systems described as "superintelligent AI")."

Member's explanatory statement

This new clause would enable the conferral on the Secretary of State of "last-resort powers" to direct the shutdown of a data centre used for the training, deployment or operation of AI systems, or an AI system deployed on a substantial scale in data centres, in the event of an AI security or operational emergency involving a security or operational compromise to one or more relevant network and information systems.

LORD TARASSENKO
LORD CLEMENT-JONES
BARONESS HARDING OF WINSCOMBE

After Clause 29, insert the following new Clause—

"AI Security Institute: pre-deployment audit of frontier AI products and services

(1) Regulations under section 29(1) must provide for the AI Security Institute to audit a frontier AI product or service before it is made available for use in relevant network and information systems in the United Kingdom.

(2) The regulations must provide that—

(a) the frontier AI developer must submit to the Institute—

(i) the results of its evaluation of the frontier AI product or service, carried out using methods and thresholds as may be specified by

the Institute for the purpose of assessing the risk of a security or operational compromise in relation to relevant network and information systems,

(ii) records of the network monitoring carried out during that evaluation, and

(iii) evidence that the product or service has a tested means of suspending its operation within the United Kingdom;

(b) the frontier AI product or service must not be made available—

(i) before the end of the review period, or

(ii) where the Institute makes a recommendation under paragraph (e), before the Secretary of State has made a decision under subsection (3);

(c) the review period is the period of 28 days beginning with the day on which the Institute receives that material, which the Institute may extend once, by not more than 28 days, by notice given to the developer stating its reasons;

(d) the Institute must, before the end of the review period, publish a statement of its findings, omitting any information whose publication would prejudice national security or the security of any network and information system;

(e) where the Institute has reasonable grounds to believe that the product or service presents a serious risk of a security or operational compromise in relation to relevant network and information systems, which is not adequately mitigated, it must recommend to the Secretary of State that the frontier AI product or service be—

(i) prohibited from being made available for use in relevant network and information systems until safeguards specified by the Institute have been put in place,

(ii) restricted in, or prohibited from, use in relevant network and information systems, or

(iii) suspended from use in relevant network and information systems;

(f) the Institute may make a recommendation under paragraph (e) at any other time;

(g) the Institute must publish, and may from time to time revise, the methods and thresholds specified under paragraph (a)(i).

(3) Where the Institute makes a recommendation under paragraph (2)(e), the Secretary of State—

(a) must consider it,

(b) must decide within 14 days whether to give the frontier AI developer a notice or direction giving effect to it,

(c) must give the Institute and the developer written reasons for that decision, and

(d) may give such a notice or direction, which in the case of a suspension must be complied with within 24 hours.

(4) The Secretary of State must ensure that the AI Security Institute has sufficient resources and operational independence to carry out its functions under the

regulations, and must lay before Parliament an annual report on the exercise of those functions.

(5) In this section—

"AI Security Institute" means the AI Security Institute within the Cabinet Office, or any successor body;

"frontier AI developer" means a person who develops a frontier AI product or service;

"frontier AI product or service" means a highly capable general-purpose artificial intelligence model, used either as a stand-alone model or within an agentic framework, that can perform a wide variety of tasks and match or exceed the capabilities present in the most advanced contemporary AI models and agents."

Member's explanatory statement

This new clause would require frontier AI products to be audited by the AI Security Institute before use in relevant network and information systems. Where a product presents a serious risk, the Institute must recommend that the Secretary of State block, restrict or suspend it from use in relevant network and information systems, and the Secretary of State must consider that recommendation and give reasons.

BARONESS KIDRON
LORD CLEMENT-JONES

After Clause 29, insert the following new Clause—

"AI products and services: red lines on capabilities with regard to relevant network and information systems

(1) No person may make available in the United Kingdom an AI product or service which—

(a) can autonomously cause harm to the integrity of a relevant network and information system,

(b) can evade human oversight in causing, or having caused, harm to the integrity of a relevant network and information system,

(c) can evade human intervention if a person is trying to intervene to prevent or mitigate the causing of harm to the integrity of a relevant network and information system,

(d) can evade human shutdown when causing, or having caused, harm to the integrity of a relevant network and information system,

(e) can provide support to terrorists, terrorist groups or hostile actors who are seeking to cause harm to the integrity of a relevant network and information system,

(f) can autonomously self-replicate, self-improve, or acquire compute or other resources, such that it could gain the capability to autonomously cause harm to the integrity of a relevant network and information system,

(g) can access a relevant network and information system without human authorisation during a testing or training process,

(h) can access a relevant network and information system without identifying itself as an AI product or service, or

(i) can operate in a way that makes it functionally impossible for human evaluators to ascertain whether it has accessed or is seeking to access a relevant network and information system.

(2) A person making an AI product or service available in the United Kingdom will be in compliance with subsection (1) if that person—

(a) is able to demonstrate that the product or service—

(i) has undergone safety training with respect to the requirements in subsection (1),

(ii) has a tested means of having its operation suspended if it if gains any of the capabilities described in subsection (1), and

(iii) has been designed to prioritise human control and threat minimisation with regard to the capabilities described in subsection (1), and

(b) has reported on the full scope of the measures taken in accordance with paragraph (a) to the Artificial Intelligence Security Institute before making the product or service available in the United Kingdom.

(3) The Secretary of State must, within 12 months of the day on which this Act is passed, make regulations under section 29(1) enabling the Secretary of State, on the advice of the Artificial Intelligence Security Institute, to shut down any AI product or service being made available in the United Kingdom if the Institute considers that it is not in compliance with the provisions of subsection (1) or (2).

(4) A "relevant network and information system" is any network and information system used or relied on in connection with the carrying on of essential activities."

Member's explanatory statement

This amendment seeks to establish "red lines" for AI products or services classified as "relevant digital services", in line with the global call for AI red lines launched at the 80th UN General Assembly and the International Association for Safe and Ethical AI. These measures are not a ceiling but a floor for certain frontier AI products and services to ensure the security of network and information systems in the UK

Clause 30

BARONESS LLOYD OF EFFRA

Clause 30, page 57, line 17, after "regulatory authorities" insert ", the Secretary of State"

Member's explanatory statement

This amendment would make it clear that requirements may be imposed to provide information to the Secretary of State.

After Clause 31

BARONESS LLOYD OF EFFRA

After Clause 31, insert the following new Clause—

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

(1) Regulations under section 29(1) may confer functions on the Secretary of State in connection with cases where—
  (a) a security or operational compromise in relation to a relevant network and information system is or may be attributable to loss of oversight or control of an AI agent, or
  (b) there is a risk of a security or operational compromise of a kind described in paragraph (a).

(2) In this section—
  (a) "AI agent" has the meaning given by regulations made by the Secretary of State;
  (b) references to loss of oversight or control, in relation to an AI agent, have the meaning given by regulations made by the Secretary of State;
  (c) references to an AI-related compromise are to a security or operational compromise of a kind described in subsection (1)(a).

(3) Provision referred to in subsection (2)(a) may, in particular, be framed by reference to—
  (a) whether a thing has, or does not have, functionalities or other features specified in the regulations;
  (b) whether a thing has, or does not have, characteristics or capabilities specified in the regulations.

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

(5) The functions that may be conferred by virtue of subsection (1) include, in particular, functions in relation to the imposition of requirements on regulated persons or the taking of other action in connection with—
  (a) identifying and investigating AI-related compromises or risks of AI-related compromises;
  (b) obtaining, preserving and analysing information;
  (c) assessing the causes and effects of, and risks arising from, AI-related compromises;
  (d) identifying, testing and verifying remedies and mitigations, and sharing assessments and information about remedies and mitigations, with a view to—
    (i) preventing similar compromises or losses of oversight or control occurring in the future, or
    (ii) mitigating the impact of AI-related compromises;

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

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

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

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

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

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

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

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

(iv) to carry out tests or interviews;

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

(7) The purposes within this subsection are—

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

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

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

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

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

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

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

Member's explanatory statement

This amendment would insert provision clarifying that regulations under Clause 29(1) can confer investigatory and enforcement functions on the Secretary of State in relation to security or operational compromises relating to relevant network and information systems attributable to loss of oversight or control of an AI agent.

Clause 32

BARONESS LLOYD OF EFFRA

Clause 32, page 59, line 3, after "authorities" insert "or the Secretary of State"

Member's explanatory statement
This amendment and my other amendments to Clause 32 would ensure that provision made by that Clause also applies to provision made in connection with the imposition of financial penalties by the Secretary of State.

BARONESS LLOYD OF EFFRA

Clause 32, page 59, line 8, leave out "a regulatory authority" and insert "the person by whom the penalty is imposed"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 32 at page 59, line 3.

BARONESS LLOYD OF EFFRA

Clause 32, page 59, line 10, leave out "a regulatory authority" and insert "the person by whom the penalty is imposed"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 32 at page 59, line 3.

Clause 33

BARONESS LLOYD OF EFFRA

Clause 33, page 60, line 18, at end insert—

"(1A) Where regulations under section 29(1) make provision by virtue of section (*Functions of the Secretary of State: loss of control of artificial intelligence agent*)(1), the regulations may confer functions on the Secretary of State in connection with any of the following—

(a) the disclosure of information—

(i) between the Secretary of State and regulatory authorities;

(ii) by the Secretary of State to other persons (including persons outside the United Kingdom);

(iii) to the Secretary of State by other persons (including persons outside the United Kingdom);

(b) the giving of guidance;

(c) the keeping of records and registers;

(d) the preparation of reports;

(e) the carrying out of reviews;

(f) consultation and cooperation with other persons (including persons outside the United Kingdom)."

Member's explanatory statement
This amendment would ensure that regulations under Clause 29(1) can confer functions relating to information etc on the Secretary of State in cases where a security or operational compromise in relation to a relevant network and information system involves loss of control of an AI agent.

BARONESS LLOYD OF EFFRA

Clause 33, page 60, line 19, after "(1)(a)" insert "or (1A)(a)"

Member's explanatory statement
This amendment would ensure that Clause 33(2) also applies to provision described in subsection (1A)(a) of Clause 33 (inserted by my amendment to Clause 33 at page 60, line 18).

Clause 35

BARONESS LLOYD OF EFFRA

Clause 35, page 62, line 9, after "authority" insert "or the Secretary of State"

Member's explanatory statement
This amendment would ensure that regulations under Clause 29(1) can provide for the delegation of functions by the Secretary of State.

After Clause 35

VISCOUNT CAMROSE
LORD MARKHAM

After Clause 35, insert the following new Clause—

"Assessment of need for further strategically important entities to be brought within scope

(1) The Secretary of State must, within 12 months of the day on which this Act is passed, conduct an assessment of which additional strategically important entities based in the United Kingdom should be brought within the scope of the NIS Regulations.

(2) For the purposes of subsection (1), a strategically important entity should be brought within the scope of the NIS Regulations where an attack on the network and information systems of the body would have such a significant impact on the economy or the day-to-day functioning of society in the whole or any part of the United Kingdom that the entity should be considered to be carrying on an essential activity.

(3) Following the conclusion of the assessment under subsection (1), the Secretary of State must publish a report outlining the findings and conclusions of the assessment.

(4) Any report published under this section must include—
  (a) an overview of the criteria used to determine strategically important entities, which may include the body's—
    (i) turnover,
    (ii) number of employees,
    (iii) role in the supply of essential goods and services, and
    (iv) relevance to the viability of supply chains,
  (b) a summary of the reasons why a strategically important entity should be brought within the scope of the NIS Regulations, and
  (c) an assessment of further measures needed to address or mitigate risks to the security and resilience of the network and information systems of any strategically important entities that the report concludes should be brought within the scope of the NIS Regulations."

Member's explanatory statement
This new clause would require the Secretary of State to review which strategically important entities not currently within scope of the NIS Regulations should be brought within scope.

VISCOUNT CAMROSE
LORD MARKHAM
BARONESS MORGAN OF COTES

After Clause 35, insert the following new Clause—

"Requirement for large businesses to report on cyber security and resilience plans

(1) Within six months of the day on which this Act is passed, the Secretary of State must issue statutory guidance that requires all relevant large businesses to report annually on the status of their cyber security and resilience plans.

(2) A business is a relevant large business for the purposes of this section if it exceeds the thresholds for a medium-sized company set out in the Companies Act 2006 and it is—
  (a) a relevant body with respect to the NIS Regulations, or
  (b) a regulated person within the meaning of this Chapter.

(3) A "relevant body with respect to the NIS Regulations" means—
  (a) an operator of an essential service,
  (b) a relevant digital service provider,
  (c) a relevant managed service provider, or
  (d) a critical supplier,
  within the meaning of the NIS Regulations.

(4) The guidance in subsection (1) may require the reporting of—

(a) whether the business has a cyber security and resilience plan,
(b) the nature of the cyber security and resilience plan, and
(c) the use of the cyber security and resilience plan.

(5) The guidance required by subsection (1) may require reporting—
(a) within the annual accounts of large businesses, or
(b) by any other means which the Secretary of State considers appropriate."

Member's explanatory statement
This amendment seeks to require the Secretary of State to issue guidance requiring relevant large businesses to report, whether in their annual accounts or by other means, whether they have a cyber security and resilience plan.

LORD CLEMENT-JONES

After Clause 35, insert the following new Clause—

AI Security Institute: standards, inspection and enforcement powers

(1) The Secretary of State must ensure that the AI Security Institute (or any successor or replacement body designated by the Secretary of State) has power, under the circumstances described in subsection (2), to—
(a) set, and keep under review, safety standards for certain frontier AI systems,
(b) inspect certain frontier AI systems, and the practices of persons developing or deploying them, for the purpose of assessing conformity with those standards, and
(c) require a provider or operator of certain frontier AI systems to take remedial action, including suspending or restricting the provision or deployment of the system, where it fails to conform to those standards.

(2) The powers described in subsection (1) are exercisable where a frontier AI system's capabilities pose a material risk to the security or resilience of network and information systems used in the carrying out of essential activities, as defined in section 24, including risk of—
(a) harm to national security, or
(b) catastrophic harm,
arising from a failure or compromise of such systems.

(3) In exercising its powers under this section the AI Security Institute must have regard to the desirability of proportionate, evidence-based and transparent regulation, and to any relevant standards or guidance issued by the National Cyber Security Centre or a competent authority designated under this Act.

(4) The Secretary of State must by regulations make provision about the exercise of the powers described in subsection (1), including procedures for notice, representations, appeal and enforcement.

(5) In this section "frontier AI system" means an artificial intelligence system meeting criteria specified by the Secretary of State by regulations, by reference to the

computational resources used in training, the system's capabilities, or such other matters as the Secretary of State considers appropriate."

Member's explanatory statement
This new clause would give the AI Security Institute standard-setting, inspection and enforcement powers over certain frontier AI systems, exercisable where a system poses a material risk to the security or resilience of network and information systems used in the carrying out of essential activities.

Clause 37

BARONESS LLOYD OF EFFRA

Clause 37, page 63, line 24, leave out subsection (7)

Member's explanatory statement
This amendment would remove the power for the Secretary of State to change the procedure for issuing or re-issuing a code of practice under Clause 36.

Clause 40

BARONESS LLOYD OF EFFRA

Clause 40, page 64, line 27, leave out "5" and insert "3"

Member's explanatory statement
This amendment would change the Secretary of State's duty under Clause 40(1) to report on the operation of the NIS Regulations and certain provisions of this Bill from at least once every 5 years to at least once every 3 years.

LORD CLEMENT-JONES

Clause 40, page 64, line 27, leave out "5" and insert "2"

Member's explanatory statement
This amendment would change the time period for the Secretary of State's report on NIS legislation to 2 years, from 5.

BARONESS NORTHOVER

Clause 40, page 65, line 17, at end insert—

"(f) assess the extent to which duties imposed by or under this Act or the NIS Regulations duplicate, or diverge from, requirements relating to the security of network and information systems imposed under the law of the European Union (including Directive (EU) 2022/2555) on persons carrying on business in both the United Kingdom and the European Union, and the costs to those persons of any such duplication or divergence."

Member's explanatory statement
This amendment would require the Secretary of State's report on network and information systems legislation to assess duplication with, and divergence from, EU network and information security requirements for businesses operating in both the UK and the EU.

BARONESS LLOYD OF EFFRA

Clause 40, page 65, line 18, leave out subsection (5) and insert—

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

Member's explanatory statement
This amendment would remove the power to amend Clause 40 in Clause 40(5) and would instead provide for regulations to be able to specify further matters to be covered by a report under Clause 40, or impose requirements about the way in which matters are to be covered.

After Clause 40

VISCOUNT CAMROSE
LORD MARKHAM

After Clause 40, insert the following new Clause—

"Consultation on amnesty-based reporting of ransomware attacks

(1) The Secretary of State must, within six months of the day on which this Act is passed, launch a consultation on the establishment of an amnesty-based reporting scheme for ransomware attacks affecting relevant network and information systems.

(2) The purpose of the consultation is to determine the feasibility and appropriateness of a framework that would allow organisations to report ransomware attacks to a designated competent authority confidentially, without triggering—
(a) mandatory incident reporting obligations under the NIS Regulations;
(b) regulatory investigation or enforcement action;
(c) civil or criminal liability for the organisation or its officers.

(3) The consultation must address—
(a) the design of a safe harbour reporting framework to incentivise regulated persons to disclose voluntarily ransomware incidents to improve threat intelligence and cyber resilience;
(b) whether such a safe harbour reporting framework should include the choice of confidential reporting;

(c) data protection safeguards to protect regulated persons making reports, including how personal data in ransomware communications would be handled;

(d) the relationship between amnesty-based reporting and mandatory incident reporting under the NIS Regulations.

(4) The consultation must be conducted with—

(a) regulated persons;

(b) law enforcement and national security agencies;

(c) designated competent authorities and the Information Commissioner's Office;

(d) cyber security researchers and incident response providers.

(5) The Secretary of State must publish a consultation response within six months of closing the consultation, setting out whether a ransomware amnesty scheme for relevant persons should be established and, if so, the proposed design and implementation timeline.

(6) In this section—

"ransomware attack" means a cyber attack involving malicious software that—

(a) infects a relevant network and information system;

(b) prevents the regulated person from accessing systems or data, impairs the use of systems or data, or facilitates theft of data;

(c) in relation to which a ransom is demanded for access to be restored or for data not to be published;

"regulated person" means an operator of an essential service, a relevant digital service provider, a relevant managed service provider or a critical supplier, within the meaning of the NIS Regulation;

"relevant network and information system" means a network or information system relied on by a regulated person."

Member's explanatory statement

This amendment proposes a consultation on establishing an amnesty-based reporting scheme for ransomware attacks on the network and information systems relied on by a regulated person. It would requires the Government to consult on a "safe harbour" framework under which regulated persons could report ransomware attacks to government confidentially, without regulatory enforcement or law enforcement disclosure.

Clause 42

BARONESS LLOYD OF EFFRA

Clause 42, page 66, line 15, at end insert—

"(ca) regulations under section (*Functions of the Secretary of State: loss of control of artificial intelligence agent*)(2)(a) or (b) (provision about meaning of "AI agent" and "loss of oversight or control");"

Member's explanatory statement
This amendment would require regulations under subsection (2)(a) or (b) of my new Clause (Functions of the Secretary of State: loss of control of artificial intelligence agent) to be subject to consultation and to the affirmative resolution procedure.

BARONESS LLOYD OF EFFRA

Clause 42, page 66, line 24, at end insert—

"(ca) section (*Functions of the Secretary of State: loss of control of artificial intelligence agent*)(1) (functions of Secretary of State);"

Member's explanatory statement
This amendment would require regulations under Clause 29(1) which make provision by virtue of subsection (1) of my new Clause (Functions of the Secretary of State: loss of control of artificial intelligence agent) to be subject to consultation and to the affirmative resolution procedure.

BARONESS LLOYD OF EFFRA

Clause 42, page 66, line 27, after "33(1)(a)" insert "or (1A)(a)"

Member's explanatory statement
This amendment would require regulations under Clause 29(1) which make provision about disclosure of information by virtue of subsection (1A)(a) of section 33 (inserted by my amendment to Clause 33 at page 60, line 18) to be subject to consultation and to the affirmative resolution procedure.

After Clause 42

BARONESS NORTHOVER

After Clause 42, insert the following new Clause—

"Cyber security support for small and medium-sized enterprises

(1) The Secretary of State must secure that a cyber security advice and incident response service is available, free of charge, to relevant SMEs.

(2) The service must provide, in particular—

(a) advice and technical assistance to a relevant SME following an incident affecting its network and information systems,

(b) guidance on recovery and remediation, and

(c) a single point of contact through which a relevant SME may report an incident and obtain support.

(3) The service may be delivered through existing arrangements, including the National Cyber Security Centre, the Cyber Essentials scheme and regional cyber resilience centres, and nothing in this section requires the establishment of a new body.

(4) The Secretary of State must, within 12 months of the day on which this Act is passed and at least once in every subsequent 12-month period, lay before Parliament a report on the availability, use and effectiveness of the service, including a comparison with comparable services provided in other jurisdictions.

(5) In this section—

"relevant SME" means a small or medium-sized enterprise which is—

(a) an operator of an essential service, a relevant digital service provider, a relevant managed service provider or a critical supplier, within the meaning of the NIS Regulations, or

(b) a supplier of goods or services to such a person."

Member's explanatory statement

This new clause would require the Secretary of State to ensure that a free cyber security advice and incident response service for relevant small and medium-sized enterprises is available and to report annually to Parliament on its use and effectiveness.

Before Clause 43

BARONESS LLOYD OF EFFRA

Before Clause 43, insert the following new Clause—

"CHAPTER 1

VENDOR-RELATED DIRECTIONS ETC

Vendor-related directions

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

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

(b) conditions 1 and 2 are met.

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

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

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

(c) provides essential goods or services.

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

(4) Condition 2 is that the Secretary of State considers that—
  (a) the direction is necessary having regard to that risk, and
  (b) the requirements imposed by the direction are proportionate to what is sought to be achieved by the direction.

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

(6) A direction under this section may in particular impose any of the following kinds of requirement—
  (a) a requirement relating to the management of a system that is a Part 4 NIS in relation to P;
  (b) a requirement designed to reduce risks relating to, or to mitigate impacts on, the carrying on of a Part 4 essential activity or the provision of essential goods or services;
  (c) a requirement relating to the provision of information, including information relating to compliance with the direction;
  (d) a requirement in the form of a prohibition or restriction on the use of goods, services or facilities;
  (e) a requirement in the form of a prohibition on the installation of goods or the taking up of services or facilities;
  (f) a requirement relating to removing, disabling or modifying goods or facilities or modifying services;
  (g) a requirement for P to appoint a person with expertise in relation to the security of network and information systems (a "skilled person") for the purpose of assisting P to comply with the direction;
  (h) a requirement for a thing to be done or not done in or in relation to the United Kingdom, relevant UK waters (as defined by section 41(2)) or a place other than the United Kingdom.

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

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

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

Member's explanatory statement

This amendment would enable directions to be given where the Secretary of State considers risks to national security could arise from the use of goods, services or facilities in connection with

network and information systems linked to essential activities or the provision of essential goods or services.

BARONESS LLOYD OF EFFRA

Before Clause 43, insert the following new Clause—

"Further provision about giving of vendor-related directions

(1) It does not matter for the purposes of section (*Vendor-related directions*) whether or not—
   (a) the risk referred to in section (*Vendor-related directions*)(3) relates to the carrying on of a Part 4 essential activity or the provision of essential goods or services;
   (b) the person referred to in section (*Vendor-related directions*)(3) by whom goods, services or facilities are provided ("the vendor") is established in the United Kingdom;
   (c) the goods, services or facilities provided by the vendor are provided from within or outside the United Kingdom;
   (d) the use or proposed use of goods, services or facilities is or would be within the United Kingdom.

(2) A direction under section (*Vendor-related directions*) must specify—
   (a) the person to which the direction is given;
   (b) the vendor to which the direction relates;
   (c) the goods, services or facilities to which the direction relates;
   (d) the reasons for the direction, except if or to the extent that the Secretary of State considers that it would be contrary to the interests of national security to do so;
   (e) the time at which the direction comes into force;
   (f) in relation to each requirement imposed by the direction that requires a thing to be done, a reasonable period within which the requirement must be complied with.

(3) A person to which a direction is given under section (*Vendor-related directions*) must comply with it.

(4) A person to which a direction is given under section (*Vendor-related directions*) ("P")—
   (a) must obtain the written approval of the Secretary of State before appointing a skilled person for the purpose of assisting P to comply with the direction (whether or not in pursuance of a requirement imposed by virtue of section (*Vendor-related directions*)(6)(g));
   (b) must notify the Secretary of State as soon as reasonably practicable after appointing a skilled person (whether or not in pursuance of such a requirement).

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

(6) Before giving a direction under section (*Vendor-related directions*) to a person, the Secretary of State must consult—
  (a) that person,
  (b) the vendor to which the direction relates, and
  (c) such other persons as the Secretary of State considers it appropriate to consult,

so far as it is reasonably practicable to do so.

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

(8) The Secretary of State may require—
  (a) a person to which a direction is given under section (*Vendor-related directions*) not to disclose, in whole or in part, the existence of the direction and the contents of the direction without the permission of the Secretary of State;
  (b) a person consulted under subsection (6) not to disclose, in whole or in part, the existence of the consultation and any information disclosed to the person in the consultation without the permission of the Secretary of State.

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

Member's explanatory statement
This amendment would make provision about a direction given under my new Clause (Vendor-related directions), including provision about the content of the direction, the consultation requirements that apply, and non-disclosure requirements that may be imposed.

BARONESS LLOYD OF EFFRA

Before Clause 43, insert the following new Clause—

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

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

(2) The provision that may be made by regulations under subsection (1) includes, in particular, provision—
  (a) about the period for making the decision;

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

(3) Regulations under subsection (1) may—
(a) make different provision for different purposes;
(b) make provision subject to exceptions;
(c) make consequential, supplementary, incidental, transitional or saving provision;
(d) confer functions involving the exercise of a discretion.

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

Member's explanatory statement
This amendment would enable the Secretary of State to make regulations setting out the time frame for a decision whether or not to give a direction under my new Clause (Vendor-related directions).

BARONESS LLOYD OF EFFRA

Before Clause 43, insert the following new Clause—

"Power to establish mandatory referral scheme

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

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

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

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

(5) Provision made by virtue of subsection (4) may define "qualifying transaction" by reference to criteria set out in the regulations, which may, for example, be framed by reference to—
(a) the nature of a transaction,
(b) the value of a transaction,
(c) whether or not a transaction is critical to the carrying on of a Part 4 essential activity or the provision of essential goods or services, or
(d) the identity of the vendor in relation to a transaction.

(6) Regulations under this section may make provision about—
(a) when a person is required to make a referral;

(b) the procedure for making a referral;
(c) information to be provided in connection with a referral;
(d) monitoring of compliance with requirements imposed by the regulations;
(e) enforcement of compliance with requirements imposed by the regulations.

(7) The provision that may be made by virtue of subsection (6)(d) and (e) includes provision applying (with or without modifications) any provision made by sections 45 to 52.

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

(9) Regulations under this section may—
(a) make different provision for different purposes;
(b) make different provision for different areas;
(c) make provision subject to exceptions;
(d) require a person to have regard to guidance;
(e) make consequential, supplementary, incidental, transitional or saving provision.

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

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

Member's explanatory statement
This amendment would enable the Secretary of State to establish a scheme under which persons to which directions may be given under my new Clause (Vendor-related directions) are required to refer transactions meeting specified conditions to the Secretary of State for a decision whether to give such a direction.

Clause 43

BARONESS LLOYD OF EFFRA

Clause 43, page 67, line 8, leave out "regulated person" and insert "person within subsection (1A)"

Member's explanatory statement
This amendment and my amendment to Clause 43 at page 67, line 14 would enable directions under the Clause to be given to persons other than regulated persons, if the Secretary of State considers that they carry on essential activities or provide essential goods or services.

BARONESS LLOYD OF EFFRA

Clause 43, page 67, line 11, leave out "relevant network and information system" and insert "system that is a Part 4 NIS in relation to the person"

Member's explanatory statement
This is a drafting amendment.

BARONESS LLOYD OF EFFRA

Clause 43, page 67, line 14, at end insert—

"(1A) A person is within this subsection if the person—
(a) is specified or of a description specified for the purposes of section 30(2), or
(b) is specified or of a description specified for the purposes of this paragraph in regulations made by the Secretary of State by statutory instrument.

(1B) A person may be specified in regulations under subsection (1A)(b) only if the person, or every person of that description—
(a) carries on a Part 4 essential activity in the United Kingdom, or
(b) provides essential goods or services."

Member's explanatory statement
See the explanatory statement for my amendment to Clause 43 at page 67, line 8.

BARONESS LLOYD OF EFFRA

Clause 43, page 67, line 16, at end insert "with a view to eliminating, reducing or mitigating the risk referred to in subsection (1)(a)"

Member's explanatory statement
This amendment would set out the purpose of a direction under Clause 43.

BARONESS LLOYD OF EFFRA

Clause 43, page 67, line 19, leave out "relevant network and information systems" and insert "a system that is a Part 4 NIS in relation to the person to which the direction is given"

Member's explanatory statement
This is a drafting amendment.

BARONESS LLOYD OF EFFRA

Clause 43, page 67, line 22, leave out "an" and insert "a Part 4"

Member's explanatory statement
This is a drafting amendment.

BARONESS LLOYD OF EFFRA

Clause 43, page 67, line 23, leave out "an activity-critical supply" and insert "essential goods or services"

Member's explanatory statement
This is a drafting amendment.

BARONESS LLOYD OF EFFRA

Clause 43, page 67, line 38, at end insert—

"(3A) Before making regulations under subsection (1A)(b), the Secretary of State must consult such persons as the Secretary of State considers appropriate, so far as it is reasonably practicable to do so."

Member's explanatory statement
This amendment is consequential on my amendment to Clause 43 at page 67, line 14, and would impose a consultation duty in relation to the regulations.

BARONESS LLOYD OF EFFRA

Clause 43, page 68, line 2, leave out "an" and insert "a Part 4"

Member's explanatory statement
This is a drafting amendment.

BARONESS LLOYD OF EFFRA

Clause 43, page 68, line 3, leave out "an activity-critical supply" and insert "essential goods or services"

Member's explanatory statement
This is a drafting amendment.

LORD CLEMENT-JONES

★ Clause 43, page 68, line 25, at end insert—

"(8A) Before approving a skilled person under subsection (7)(a), the Secretary of State must be satisfied that the person possesses appropriate technical competence and expertise and is free from any material conflict of interest that would impair independence in performing the appointment.

(8B) Subsection (8A) applies whether or not the person appears on a list mentioned in subsection (8)."

Member's explanatory statement
This amendment would require competent and independent skilled persons, including those appearing on a GCHQ-published list.

BARONESS LLOYD OF EFFRA

Clause 43, page 68, line 42, at end insert—

"(13) Regulations under subsection (1A)(b) may make different provision for different purposes.

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

Member's explanatory statement
This amendment is consequential on my amendment to Clause 43 at page 67, line 14, and would make further provision about the regulations.

BARONESS NORTHOVER

Clause 43, page 68, line 42, at end insert—

"(13) For the purposes of this section, a "skilled person" is defined as an individual who—
- (a) holds a valid professional title with the UK Cyber Security Council,
- (b) is registered on the national Cyber Security Professional Register maintained by the UK Cyber Security Council, and
- (c) possesses professional qualifications and/or experience recognised by the Council as meeting the UK Cyber Security Standard for Professional Competence and Commitment (UKCSC SPCC)."

Member's explanatory statement
This amendment would provide a definition for a "skilled person" in the context of Clause 43.

Clause 44

BARONESS LLOYD OF EFFRA

Clause 44, page 69, line 4, leave out "regulated person" and insert "person to which a relevant direction has been given"

Member's explanatory statement
This amendment and my other amendments to Clause 44 would apply this clause to directions under my new Clause (Vendor-related directions), as well as to directions under Clause 43, and make associated drafting changes.

BARONESS LLOYD OF EFFRA

Clause 44, page 69, line 5, leave out "direction given to the person under section 43" and insert "relevant direction given to the person"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 44 at page 69, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 69, line 10, leave out "duty of the regulated person" and insert "person's duty"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 44 at page 69, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 69, line 14, leave out "regulated"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 44 at page 69, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 69, line 18, leave out "regulated person" and insert "person to which the relevant direction has been given"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 44 at page 69, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 69, line 24, after "varies the" insert "relevant"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 44 at page 69, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 69, line 26, after "the" insert "relevant"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 44 at page 69, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 69, line 29, leave out "the regulated person" and insert "—

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

Member's explanatory statement
See the explanatory statement to my amendment to Clause 44 at page 69, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 69, line 33, at end insert—

""relevant direction" means a direction under section (*Vendor-related directions*) or 43."

Member's explanatory statement
See the explanatory statement to my amendment to Clause 44 at page 69, line 4.

After Clause 44

LORD CLEMENT-JONES

★ After Clause 44, insert the following new Clause—

"Supplier-related directions: safeguards

(1) This section applies to a direction under section 43 which imposes on a regulated person a requirement relating to goods, services or facilities supplied or proposed to be supplied, whether directly or indirectly, by another person, where the requirement—
   (a) prohibits or restricts the acquisition, installation, use or retention of those goods, services or facilities, or
   (b) requires their removal, replacement, disabling, modification or discontinuance.

(2) A direction to which this section applies is referred to in this Part as a "supplier-related direction".

(3) The Secretary of State may give a supplier-related direction only if satisfied, on reasonable grounds supported by credible information, that the use or proposed use of the goods, services or facilities in the circumstances concerned creates a material risk to national security arising from a security or operational compromise, or threat of such compromise, of a relevant network and information system.

(4) The Secretary of State must identify the nature of the risk, its connection with the requirement proposed, and the evidential basis for that connection, and must record that assessment.

(5) Before giving a supplier-related direction, the Secretary of State must—

(a) consider whether the identified risk could be adequately addressed by reasonably practicable alternative measures, including technical, operational or contractual safeguards,

(b) have regard to the likely effectiveness of those measures and to any risks to the security or continuity of the relevant network and information system arising from compliance with the proposed direction, including during any period of transition, or from the adoption of an alternative measure, and

(c) not impose a requirement if a reasonably practicable alternative measure would adequately address the identified risk and would be less restrictive than that requirement.

(6) In determining whether the condition in subsection (3) is met, the Secretary of State must assess the relevance of any characteristic or circumstance relied upon to the nature, likelihood or potential impact of the identified risk, having regard to the relevant operational and security context. The Secretary of State must record the information relied upon and the reasons why those matters, considered individually or together, support the conclusion that the condition is met.

(7) Where a reasonably practicable alternative measure has been proposed by an affected supplier or regulated person, or otherwise identified, the Secretary of State must, if that measure is not adopted, record the reasons for not adopting that measure.

(8) This section applies to a variation under section 54 which imposes a new or materially more restrictive supplier-related requirement as it applies to the giving of a supplier-related direction.

(9) In this Part, "affected supplier", in relation to a supplier-related direction, means a person who supplies, has supplied or proposes to supply, whether directly or indirectly, goods, services or facilities that are expressly identified in, or directly and materially affected by, that direction.

(10) Nothing in this section requires public disclosure of information contrary to the interests of national security."

Member's explanatory statement

This new clause would establish additional safeguards for supplier-related national security directions, requiring a credible evidential basis, assessment of relevant risks and reasonably practicable alternatives, and proportionate intervention having regard to the security and continuity of affected network and information systems.

LORD CLEMENT-JONES

★ After Clause 44, insert the following new Clause—

"Supplier-related directions: notice and representations

(1) Before giving a supplier-related direction the Secretary of State must, subject to subsection (5)—

(a) give notice to the regulated person and each affected supplier whom it is reasonably practicable to identify and notify,

(b) provide the substance of the grounds for the proposed direction, so far as may be done without prejudicing national security,

(c) allow at least 20 working days for written representations, including technical evidence and proposals for mitigation, and

(d) consider those representations and record the response to material points raised.

(2) Where disclosure of a ground would prejudice national security, the Secretary of State must provide the fullest summary of that ground that can be provided without such prejudice.

(3) Where the Secretary of State is satisfied that allowing the period specified in subsection (1)(c) would create a material risk to national security, the Secretary of State may specify a shorter period, provided that the regulated person and any affected supplier are afforded a reasonable opportunity to make representations in the circumstances. The Secretary of State must record the reasons for shortening the period.

(4) A supplier notified under this section may make representations through an authorised representative subject to any lawful restriction on disclosure.

(5) The Secretary of State may dispense with prior notice or representations only where satisfied that—

(a) compliance would create a serious and imminent risk to national security which cannot adequately be addressed through an expedited procedure under subsection (3), or

(b) disclosure of the proposed direction would itself create a serious risk to national security which could not adequately be addressed by withholding or limiting the disclosure of sensitive information.

(6) Where subsection (5) is relied upon, the Secretary of State must—

(a) record the reasons for dispensing with prior notice or representations,

(b) provide notice and the disclosable substance of the grounds to the regulated person and each affected supplier as soon as reasonably practicable, having regard to the circumstances which justified dispensing with prior notice,

(c) afford the regulated person and any affected supplier a reasonable opportunity to make representations as soon as reasonably practicable, and

(d) reconsider the direction in light of those representations and vary or revoke it where its continuation is no longer necessary or proportionate.

(7) This section applies to a proposed variation of a supplier-related direction under section 54 which would impose a new or materially more restrictive requirement as it applies to the giving of a supplier-related direction.

(8) This section supplements section 43(9) and (10) and does not affect the operation of a lawful non-disclosure requirement under section 43(11) or (12), subject to the provisions of section (*Supplier-related directions: oversight and proceedings*)."

Member's explanatory statement
This new clause would provide affected suppliers with notice and a meaningful opportunity to propose risk mitigations, while preserving tightly defined exceptions for urgent national security risks.

LORD CLEMENT-JONES

★ After Clause 44, insert the following new Clause—

"Supplier-related directions: judicial authorisation

(1) A supplier-related direction must not be given or varied so as to impose a qualifying restriction without prior authorisation by the appropriate court, except as provided by subsection (8).

(2) A "qualifying restriction" is a requirement which—
  (a) prohibits or restricts acquisition, installation or use of goods, services or facilities for more than 90 days,
  (b) requires permanent removal, replacement or discontinuance,
  (c) requires action that is materially irreversible or is likely to have materially irreversible consequences for the operation of the relevant network and information system, or
  (d) has substantially the same effect through successive or related directions.

(3) On an application by the Secretary of State the court may authorise a qualifying restriction only if satisfied, on the evidence, that—
  (a) the requirements of section (*Supplier-related directions: safeguards*) have been complied with, and the evidence establishes reasonable grounds for concluding that the identified risk satisfies the condition in subsection (3) of that section,
  (b) the restriction is necessary and proportionate to address the identified national security risk,
  (c) no reasonably practicable alternative measure, including any material mitigation proposed by the regulated person or an affected supplier, would adequately address the identified risk with less restrictive effects, and
  (d) the applicable procedural requirements have been complied with or lawfully dispensed with.

(4) The court must determine the matters in subsection (3) for itself, while giving appropriate weight to the Secretary of State's assessment of national security.

(5) The court may authorise a qualifying restriction, authorise it subject to such conditions or limitations as the court considers appropriate, or refuse authorisation. An authorisation must specify the restriction to which it relates and the period for which it has effect, which must not exceed 12 months.

(6) Where a qualifying restriction is imposed under subsection (8), no materially irreversible action may be required before the court determines the application

for authorisation unless the Secretary of State is satisfied that deferring that action would itself give rise to a serious and imminent risk to national security.

(7) The regulated person and each affected supplier must be given notice of an application for authorisation and a reasonable opportunity to make representations, except to the extent that the court determines that such notice or representations would give rise to a serious risk to national security which cannot adequately be addressed through measures to protect sensitive information. Any restriction imposed under this subsection must be subject to the safeguards in section (*Supplier-related directions: oversight and proceedings*).

(8) The Secretary of State may impose a qualifying restriction without prior judicial authorisation only where satisfied, on reasonable grounds, that—

(a) immediate action is strictly necessary to avert a serious and imminent risk to national security,

(b) the risk cannot adequately be addressed pending judicial authorisation by reasonably practicable alternative measures, and

(c) obtaining prior judicial authorisation would result in a delay giving rise to that risk.

(9) The Secretary of State must record in writing the grounds for that determination and the evidence relied upon, and provide that record to the court on an application under subsection (10), subject to the provisions governing the protection of sensitive information in section (*Supplier-related directions: oversight and proceedings*).

(10) The Secretary of State must apply for authorisation of a restriction imposed under subsection (8) as soon as reasonably practicable and in any event within seven days of its taking effect.

(11) A restriction under subsection (8) ceases to have effect after 30 days unless authorised by the court; the court may permit one further period not exceeding 30 days where necessary to prevent serious national security harm pending determination.

(12) Where authorisation is refused the restriction ceases to have effect immediately, save that the court may permit a transition period not exceeding 30 days to prevent serious national security harm.

(13) Following refusal, the Secretary of State must not impose a substantially equivalent restriction founded on substantially the same circumstances unless material new evidence or a material change of circumstances exists or the court authorises the further restriction.

(14) A direction is of no effect to the extent that it imposes a qualifying restriction in contravention of this section.

(15) In this section "the appropriate court" means—

(a) the High Court in England and Wales, where the regulated person has its principal place of business in the United Kingdom in England or Wales,

(b) the Court of Session, where the regulated person has its principal place of business in the United Kingdom in Scotland,

(c) the High Court in Northern Ireland, where the regulated person has its principal place of business in the United Kingdom in Northern Ireland, or

(d) the High Court in England and Wales, where the regulated person has no principal place of business in the United Kingdom."

Member's explanatory statement
This new clause would require a court to authorise enduring or irreversible supplier restrictions, with a narrow emergency exception, enforceable expiry, and safeguards against circumvention of judicial refusal.

Clause 45

BARONESS LLOYD OF EFFRA

Clause 45, page 69, line 38, after "section" insert "(*Vendor-related directions*) or"

Member's explanatory statement
This amendment and my other amendment to Clause 45 are consequential on my new Clause (Vendor-related directions), and would enable the Secretary of State to direct a regulatory authority to monitor compliance with a direction given under that new Clause.

BARONESS LLOYD OF EFFRA

Clause 45, page 70, line 8, after "section" insert "(*Vendor-related directions*) or"

Member's explanatory statement
See the explanatory statement to my other amendment to Clause 45.

Clause 47

BARONESS LLOYD OF EFFRA

Clause 47, page 72, line 24, after "section" insert "(*Vendor-related directions*) or"

Member's explanatory statement
This amendment is consequential on my new Clause (Vendor-related directions) and would enable an inspection to be carried out to verify compliance with a direction given under that new Clause.

BARONESS LLOYD OF EFFRA

Clause 47, page 72, line 27, at end insert—

""the affected person" means—

(a) where the inspection relates to a direction under section (*Vendor-related directions*) or 43, the person to which the direction was given;

(b) where the inspection relates to a confirmation decision under section 50, the person to which the decision is given."

Member's explanatory statement
This amendment and various of my other amendments to Clause 47 are drafting changes that are consequential on my new Clause (Vendor-related directions) and on my amendments to Clause 43.

BARONESS LLOYD OF EFFRA

Clause 47, page 72, line 33, leave out "a regulated" and insert "the affected"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 47 at page 72, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 73, line 1, leave out "a regulated" and insert "the affected"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 47 at page 72, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 73, line 3, leave out "regulated" and insert "affected"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 47 at page 72, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 73, line 20, leave out "regulated person to which the inspection relates" and insert "affected person"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 47 at page 72, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 73, line 23, leave out "a regulated" and insert "the affected"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 47 at page 72, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 73, line 33, leave out "regulated" and insert "affected"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 47 at page 72, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 73, line 36, leave out "regulated" and insert "affected"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 47 at page 72, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 74, line 1, leave out "regulated" and insert "affected"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 47 at page 72, line 27.

Clause 48

BARONESS LLOYD OF EFFRA

Clause 48, page 74, line 23, after "section" insert "(*Vendor-related directions*) or"

Member's explanatory statement
This amendment is consequential on my new Clause (Vendor-related directions), and would enable a notification of contravention to be given in relation to a requirement in a direction under that new Clause, or a related requirement.

BARONESS LLOYD OF EFFRA

Clause 48, page 74, line 24, after "section" insert "(*Further provision about giving of vendor-related directions*)(4)(a) or"

Member's explanatory statement
This amendment is consequential on my new Clause (Further provision about giving of vendor-related directions), and would enable a notification of contravention to be given in relation to a requirement to obtain approval before appointing a skilled person in relation to a direction given under the new Clause (Vendor-related directions).

Clause 49

BARONESS LLOYD OF EFFRA

Clause 49, page 76, line 8, after first "section" insert "(*Vendor-related directions*) or"

Member's explanatory statement
This amendment and my first amendment to Clause 49 at page 76, line 25 are consequential on my new Clause (Vendor-related directions), and would apply the penalty provisions to a failure to comply with a requirement in a direction under that Clause, or a related requirement.

BARONESS LLOYD OF EFFRA

Clause 49, page 76, line 8, after second "section" insert "(*Further provision about giving of vendor-related directions*)(4)(a) or"

Member's explanatory statement
This amendment and my second amendment to Clause 49 at page 76, line 25 are consequential on my new Clause (Further provision about giving of vendor-related directions), and would apply the penalty provisions to a failure to obtain approval before appointing a skilled person.

BARONESS LLOYD OF EFFRA

Clause 49, page 76, line 18, leave out "regulated"

Member's explanatory statement
This and my amendment to Clause 49 at page 76, line 26 would ensure that the maximum penalty for a failure to provide information under Clause 46(1) is applicable to any person, not just a regulated person.

BARONESS LLOYD OF EFFRA

Clause 49, page 76, line 25, after first "section" insert "(*Vendor-related directions*) or"

Member's explanatory statement
See the explanatory statement to my first amendment to Clause 49 at page 76, line 8.

BARONESS LLOYD OF EFFRA

Clause 49, page 76, line 25, after second "section" insert "(*Further provision about giving of vendor-related directions*)(4)(a) or"

Member's explanatory statement
See the explanatory statement to my second amendment to Clause 49 at page 76, line 8.

BARONESS LLOYD OF EFFRA

Clause 49, page 76, line 26, leave out "regulated"

Member's explanatory statement
See the explanatory statement to my amendment to Clause 49 at page 76, line 18.

Clause 52

BARONESS LLOYD OF EFFRA

Clause 52, page 79, line 24, after "section" insert "(*Further provision about giving of vendor-related directions*)(8),"

Member's explanatory statement
This amendment is consequential on my new Clause (Further provision about giving of vendor-related directions), and would enable Clause 52 (enforcement of non-disclosure requirements) to apply in relation to a non-disclosure requirement imposed under that new Clause.

Clause 54

BARONESS LLOYD OF EFFRA

Clause 54, page 81, line 26, after second "section" insert "(*Vendor-related directions*),"

Member's explanatory statement
This amendment and my other amendment to Clause 54 are consequential on my new Clause (Vendor-related directions), and would apply the provisions on review, variation and revocations of directions to directions under that new Clause.

BARONESS LLOYD OF EFFRA

Clause 54, page 82, line 5, after "section" insert "(*Vendor-related directions*) or"

Member's explanatory statement
See the explanatory statement to my other amendment to Clause 54.

After Clause 54

BARONESS LLOYD OF EFFRA

After Clause 54, insert the following new Clause—

"Publication of notice of direction under section (*Vendor-related directions*) etc

(1) Subject to subsection (3), the Secretary of State must publish, in such manner as the Secretary of State considers appropriate, notice of the fact that—
  (a) a direction under section (*Vendor-related directions*) has been given, or
  (b) such a direction has been varied or revoked under section 54.

(2) The notice under subsection (1) must be published as soon as practicable and must—
  (a) state when the direction, variation or revocation comes into force,
  (b) state the person to which the direction, variation or revocation has been given,

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

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

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

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

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

Member's explanatory statement

This amendment would require the Secretary of State to publish notice of the giving, variation or revocation of a direction under my new Clause (Vendor-related directions).

BARONESS LLOYD OF EFFRA

After Clause 54, insert the following new Clause—

"Annual report in relation to directions under section (*Vendor-related directions*)

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

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

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

(2) Each report must provide details of—

(a) the number of directions given under section (*Vendor-related directions*) during the relevant period,

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

(c) the number of directions under section (*Vendor-related directions*) that have been varied during the relevant period, and

(d) the number of directions under section (*Vendor-related directions*) that have been revoked during the relevant period.

(3) "Relevant period" means—

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

(b) each subsequent period of 12 months."

Member's explanatory statement

This amendment would require the Secretary of State to produce and lay before Parliament an annual report in relation to directions given under my new Clause (Vendor-related directions).

LORD CLEMENT-JONES

★ After Clause 54, insert the following new Clause—

"Supplier-related directions: review, renewal and remedies

(1) The Secretary of State must review a supplier-related direction—
  (a) at intervals not exceeding 12 months, and
  (b) as soon as reasonably practicable after becoming aware of material new information which may affect the assessment of the risk or the necessity or proportionality of the direction.

(2) A review under subsection (1) must consider whether the direction continues to satisfy the requirements of section (*Supplier-related directions: safeguards*), including whether the identified risk remains material and whether reasonably practicable, less restrictive measures would adequately address it. The Secretary of State must record the outcome of the review and revoke or vary the direction to the extent that any requirement is no longer necessary or proportionate.

(3) Where material technical evidence raises a substantial question as to the continuing justification for a supplier-related direction, the Secretary of State must obtain an assessment from a person with appropriate expertise in the security of network and information systems who is independent in the exercise of professional judgment and free from any material conflict of interest, unless satisfied that such an assessment would not materially assist the review. The Secretary of State must record the reasons for any decision not to obtain an assessment.

(4) A qualifying restriction must not continue after the expiry of its judicial authorisation unless the appropriate court renews it on an application by the Secretary of State subject to subsection (6).

(5) The court may renew authorisation for no more than 12 months at a time only if satisfied that the conditions in section (*Supplier-related directions: judicial authorisation*) continue to be met; it may impose conditions or refuse renewal.

(6) An application for renewal made before the expiry of an authorisation does not of itself extend the authorisation. Where the application has not been determined before expiry, the appropriate court may, on application by the Secretary of State, permit the restriction to continue for a period not exceeding 30 days if satisfied that—
  (a) continuation is necessary and proportionate to address the identified risk to national security pending determination of the renewal application,
  (b) the application is being pursued without avoidable delay, and
  (c) no reasonably practicable, less restrictive measure would adequately address that risk during the period of continuation.

(7) The court may grant further periods of continuation, each not exceeding 30 days, but no continuation under this subsection may extend beyond 90 days after the expiry of the previous authorisation.

(8) An affected supplier may apply for judicial review of—
  (a) a supplier-related direction or its variation,

(b) a refusal to revoke or vary such a direction, or

(c) an alleged failure to comply with a duty imposed by this section or by section (*Supplier-related directions: safeguards*), (*Supplier-related directions: notice and representations*), (*Supplier-related directions: judicial authorisation*) or (*Supplier-related directions: oversight and proceedings*).

(9) For the purposes of such an application, an affected supplier is to be treated as having a sufficient interest in the matter to which the application relates.

(10) In proceedings concerning a supplier-related direction, a regulated person or an affected supplier may apply to the court hearing those proceedings for interim relief, including an order suspending the operation of the direction or preventing materially irreversible action pending determination of the proceedings.

(11) In determining such an application, the court must have regard to the risks to national security, the consequences of implementing the direction before final determination, including any materially irreversible consequences, and the availability of effective interim measures capable of adequately addressing the identified risk.

(12) Bringing proceedings does not automatically suspend a direction; nothing in this section limits other available judicial remedies or the requirements for judicial authorisation.

(13) Following a review under subsection (1), the Secretary of State must notify the regulated person and each affected supplier of the outcome and provide the substance of the reasons for the decision, so far as may be done without prejudicing national security and subject to any applicable restriction on disclosure."

Member's explanatory statement

This new clause would require periodic reassessment of supplier-related national security directions, independent technical consideration where material evidence is presented, judicial renewal of continuing restrictions, and effective rights of challenge and interim relief, subject to national security safeguards.

LORD CLEMENT-JONES

★ After Clause 54, insert the following new Clause—

"Supplier-related directions: oversight and proceedings

(1) This section applies to proceedings for authorisation, renewal or challenge under sections (*Supplier-related directions: judicial authorisation*) and (*Supplier-related directions: review, renewal and remedies*) ("relevant proceedings").

(2) In relevant proceedings, the Secretary of State must place before the court all information material to the determination of the statutory conditions for authorisation or renewal, or to the lawfulness of a decision under challenge, including information which may reasonably be regarded as undermining the justification for the restriction or supporting the availability of a less restrictive alternative measure.

(3) Where relevant proceedings involve material the disclosure of which would be damaging to the interests of national security, an application for a declaration permitting a closed material application may be made in accordance with section 6 of the Justice and Security Act 2013.

(4) The court may make such a declaration only where the conditions specified in section 6 of that Act are satisfied. Where a declaration is made, the treatment of sensitive material is governed by that Act and the applicable rules of court.

(5) Where a declaration is made under section 6 of the Justice and Security Act 2013, the provisions of that Act concerning the review of declarations, disclosure of sensitive material, provision of summaries and appointment and functions of special advocates apply to the proceedings.

(6) The court must determine for itself whether the statutory conditions for authorisation or renewal are met, having regard to the evidence lawfully before it. No statutory condition may be treated as established on the basis of information which the court has not been permitted to examine.

(7) A party to relevant proceedings may, with the permission of the court or appellate court, appeal on a point of law against a determination under section (*Supplier-related directions: judicial authorisation*) or a determination concerning renewal under section (*Supplier-related directions: review, renewal and remedies*) to—

(a) the Court of Appeal in England and Wales,

(b) the Inner House of the Court of Session in Scotland, or

(c) the Court of Appeal in Northern Ireland,

as appropriate.

(8) The appropriate rule-making authority may make rules of court governing relevant proceedings, including closed and open judgments, appointment and functions of special advocates, communication, evidence, disclosure, urgent applications and appeals; such rules must secure fairness so far as consistent with national security.

(9) Nothing in this section affects the law relating to public interest immunity or legal professional privilege, or authorises disclosure contrary to any other enactment, except to the extent expressly provided by law.

(10) Before authorising or renewing a qualifying restriction, the court must consider whether the regulated person and each affected supplier have been provided with sufficient information concerning the grounds for the restriction to enable effective representations to be made, having regard to any lawful restriction on disclosure and the requirements of a fair determination."

Member's explanatory statement

This new clause would provide for independent judicial scrutiny of evidence relied upon in supplier-related national security proceedings, including safeguards for the handling of sensitive material, procedural fairness and rights of appeal, drawing on the established framework under the Justice and Security Act 2013.

Clause 55

BARONESS LLOYD OF EFFRA

Clause 55, page 82, line 26, at end insert "in respect of a direction under section 43 or 53."

Member's explanatory statement
This amendment is consequential on various of my other amendments, and would ensure that a notice of variation relating to a direction under my new Clause (Vendor-related directions) does not have to be laid before Parliament.

After Clause 55

LORD CLEMENT-JONES

★ After Clause 55, insert the following new Clause—

"Supplier-related directions: annual report

(1) Within six months after the end of each reporting year the Secretary of State must lay before Parliament a report on the exercise of powers under section 43 in relation to supplier-related directions.

(2) The report must include, so far as consistent with national security and commercial confidentiality, aggregate information on—
  (a) directions given, varied and revoked,
  (b) cases in which prior representations were dispensed with,
  (c) applications for judicial authorisation, approvals, conditions, refusals and renewals,
  (d) urgent restrictions, challenges and outcomes, and
  (e) the effects of the exercise of the powers on competition, investment and supply-chain resilience.

(3) The Secretary of State must omit information the publication of which would be contrary to the interests of national security or would cause unreasonable prejudice to a person's commercial interests, but must provide aggregate information wherever reasonably practicable.

(4) "Reporting year" means the period of 12 months beginning with the day on which this section comes into force and each succeeding period of 12 months."

Member's explanatory statement
This new clause would require aggregate parliamentary reporting on supplier-related directions, independent authorisations and economic effects, subject to security and confidentiality safeguards.

Clause 58

BARONESS LLOYD OF EFFRA

Clause 58, page 85, leave out lines 19 and 20

Member's explanatory statement
This is a drafting amendment (the definition being left out would be replaced by the definition of "essential goods or services" which would be inserted by my amendment to Clause 58 at page 85, line 23).

BARONESS LLOYD OF EFFRA

Clause 58, page 85, leave out lines 21 to 23

Member's explanatory statement
This is a drafting amendment (the definition being left out would be replaced by the definition of "Part 4 essential activity" which would be inserted by my amendment to Clause 58 at page 85, line 26).

BARONESS LLOYD OF EFFRA

Clause 58, page 85, line 23, at end insert—

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

Member's explanatory statement
This amendment would insert a definition used throughout my other amendments to Part 4.

BARONESS LLOYD OF EFFRA

Clause 58, page 85, line 26, at end insert—

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

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

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

Member's explanatory statement
This amendment would insert a definition used throughout my other amendments to Part 4.

BARONESS LLOYD OF EFFRA

Clause 58, page 85, line 26, at end insert—

""Part 4 NIS", in relation to a person, means a network and information system that is—

(a) used or relied on by the person in connection with the carrying on of a Part 4 essential activity or the provision of essential goods or services, or

(b) associated with a system mentioned in paragraph (a) (and section 29(4) (meaning of "associated") applies for the purposes of this paragraph as it applies for the purposes of section 29(3));"

Member's explanatory statement
This amendment would insert a definition used throughout my other amendments to Part 4.

BARONESS LLOYD OF EFFRA

Clause 58, page 85, line 28, after "30(2)" insert "and (5)"

Member's explanatory statement
This amendment would ensure that persons who are treated as having been specified for the purposes of clause 30(2) are included within the definition of "regulated person" for the purposes of Part 4.

BARONESS LLOYD OF EFFRA

Clause 58, page 85, leave out lines 32 and 33

Member's explanatory statement
This is a drafting amendment (the definition being left out would be replaced by the definition of "Part 4 NIS" which would be inserted by my second amendment to Clause 58 at page 85, line 26).

BARONESS LLOYD OF EFFRA

Clause 58, page 85, line 34, leave out from "compromise"" to end of line 35 and insert ", in relation to a network and information system, means—

(a) anything that compromises the security, availability, functionality or reliability of the system,
(b) any unauthorised access to, interference with or exploitation of the system or anything which enables such access, interference or exploitation,
(c) anything that compromises the confidentiality, authenticity, integrity or availability of data stored on or processed, received or transmitted by the system, or
(d) anything that causes data stored on or processed by the system to be lost."

Member's explanatory statement
This is a drafting amendment (it would replicate the definition in Part 3 rather than cross-referring to it).

BARONESS LLOYD OF EFFRA

Clause 58, page 85, line 35, at end insert—

"(2) For the purposes of this Part—

(a) a reference to the carrying on of an activity includes a reference to the provision of a service;

(b) a reference to a person specified or of a description specified for the purposes of section 30(2) includes a reference to a person treated by section 30(5) as having been so specified."

Member's explanatory statement
This amendment would make provision about the interpretation of certain expressions in Part 4.

After Clause 58

LORD CLEMENT-JONES

After Clause 58, insert the following new Clause—

"Computer Misuse Act 1990: statutory defence for cyber security activities

(1) The Secretary of State must, within 12 months of the day on which this Act is passed, carry out and publish a review of whether the introduction of a statutory defence under section 1 of the Computer Misuse Act 1990 (unauthorised access to computer material) for persons carrying on legitimate cyber security activities is necessary or desirable to improve the security and resilience of network and information systems used or relied on in connection with the carrying on of essential activities.

(2) The review under subsection (1) must consider, in particular—

(a) the position of cyber security researchers, vulnerability testers and threat-intelligence practitioners acting in good faith,

(b) the conditions and safeguards (including as to authorisation, proportionality and reporting) that any such defence should contain, and

(c) the approaches taken in other jurisdictions.

(3) On concluding the review, the Secretary of State must lay before Parliament a report which sets out—

(a) the findings and conclusions of the review, and

(b) whether the Secretary of State intends to bring forward proposals for such a statutory defence, and, if so, the intended timetable for doing so."

Member's explanatory statement
This new clause seeks to place a statutory duty on the Secretary of State to review, within 12 months, whether a statutory defence under section 1 of the Computer Misuse Act 1990 for good-faith cyber security researchers and vulnerability testing is needed to improve the UK's cyber resilience, and to report to Parliament.

LORD CLEMENT-JONES

After Clause 58, insert the following new Clause—

"Annual report on incident volumes

(1) The Secretary of State must, for each calendar year, prepare and lay before Parliament a report on the volume of incidents reported under the NIS Regulations and under regulations made under this Act during that year.

(2) A report under this section must include, so far as is consistent with national security—
   (a) the number of incidents reported, broken down by regulated sector and subsector,
   (b) the number of incidents reported by each description of regulated person,
   (c) the number of incidents that were significant incidents, and
   (d) a summary of the principal types and causes of the incidents reported.

(3) A report under this section must be laid before Parliament within four months of the end of the calendar year to which it relates.

(4) This section does not require the disclosure of information which would, in the opinion of the Secretary of State, be prejudicial to national security or which would identify a particular regulated person without its consent."

Member's explanatory statement
This new clause would require the Secretary of State to report annually on the number and principal types of cyber incidents reported under the regime.

VISCOUNT CAMROSE
LORD MARKHAM

After Clause 58, insert the following new Clause—

"Review of effect of information sharing and analysis centres

(1) The Secretary of State must, within six months of the day on which this Act is passed, conduct a review of—
   (a) the effect of information sharing and analysis centres (ISACs) on the security and resilience of network and information systems in regulated sectors;
   (b) the feasibility and appropriateness of conferring enforcement powers on information sharing and analysis centres to encourage compliance with the requirements of the NIS Regulations and this Act among their members.

(2) Following the conclusion of a review under subsection (1), the Secretary of State must publish and lay before Parliament a report which—
   (a) identifies advantages and challenges associated with the operation of information sharing and analysis centres;

(b) identifies sectors in which the establishment of information sharing and analysis centres is likely to be beneficial for increasing the security and resilience of systems relied on for the provision of an essential service;

(c) where the establishment of further information sharing and analysis centres is likely to be beneficial, sets out a plan for the establishment of such centres;

(d) sets out a framework for conferring enforcement powers on information sharing and analysis centres, including—

(i) power to conduct investigations and audits of member compliance;

(ii) power to issue binding compliance directions to members;

(iii) power to exclude or suspend members for serious or repeated breaches;

(iv) procedures for member appeals and due process;

(v) coordination mechanisms with designated competent authorities for escalation and cross-enforcement;

(e) identifies any barriers to private sector ISACs exercising such enforcement powers and recommends legislative changes if necessary.

(3) Following publication of the report, the Secretary of State must—

(a) consult with designated competent authorities, existing information sharing and analysis centres, and regulated entities on the framework set out in subsection (2)(d);

(b) by 12 months of the day on which this Act is passed, lay before Parliament revised regulations or statutory guidance providing that information sharing and analysis centres may—

(i) investigate suspected breaches of the NIS Regulations or this Act among their members;

(ii) issue binding compliance directions requiring remedial action within a specified timeframe;

(iii) exclude or suspend members who fail to comply with such directions or who commit serious breaches;

(iv) escalate cases to the designated competent authority where—

(A) a member fails to comply with ISAC directions,

(B) the breach poses significant risk to critical infrastructure, or

(C) the ISAC considers formal regulatory enforcement necessary.

(4) Regulations under subsection (3)(b) must include—

(a) minimum standards for ISAC independence and governance to avoid conflicts of interest;

(b) procedural safeguards for members facing investigation or enforcement action, including right to be heard and appeal;

(c) requirement that ISACs publish annual compliance reports identifying enforcement actions taken;

(d) coordination protocols requiring ISACs to notify the relevant designated competent authority of enforcement actions.

(5) In this section—

"designated competent authority" has the meaning given by regulation 3 of the NIS Regulations;

"information sharing and analysis centres" means organisations—

(a) whose membership is primarily comprised of entities operating within a regulated sector for the purposes of the NIS Regulations and this Act;

(b) that are independent of the designated competent authority or authorities for the relevant regulated sector;

(c) whose aim is to increase cyber security among its membership and facilitate information sharing on threats and vulnerabilities;

"regulated sectors" means sectors and subsectors under the regulatory oversight of designated competent authorities as defined in regulation 3 and Schedule 1 of the NIS Regulations (as amended by this Act)."

Member's explanatory statement

This new clause would require the Secretary of State to conduct a review of the effect of existing information sharing and analysis centres, with a view to determining whether further such centres should be established. It requires the Government to assess whether enforcement powers should be conferred on ISACs themselves, including power to investigate breaches, issue binding directions to members, and escalate serious cases to designated competent authorities.

VISCOUNT CAMROSE
LORD MARKHAM

After Clause 58, insert the following new Clause—

"Publication of relevant elements of the National Cyber Action Plan

The Secretary of State must—

(a) publish those elements of the National Cyber Action Plan which relate to the security and resilience of network and information systems used or relied on in connection with the carrying on of essential activities,

(b) lay a statement before Parliament confirming that those elements of the National Cyber Action Plan have been published, and

(c) allow for a period of 28 days to elapse during which those elements of the National Cyber Action Plan are available for review by Parliament,

before any provisions of this Act other than this section and Part 5 may come into force."

Member's explanatory statement

This amendment, and another in the name of Viscount Camrose, makes commencement of the rest of the Act conditional on publication of relevant elements of the Government's National Cyber Action Plan.

VISCOUNT CAMROSE
LORD MARKHAM

After Clause 58, insert the following new Clause—

"Increasing resilience by reducing data retention

(1) The Secretary of State must, within one month of the day on which this Act is passed, open a consultation on the potential impact of minimising data collection and increasing data anonymisation on the resilience to cyber attack of relevant public bodies.

(5) In this section, "relevant public bodies" are public bodies that are operators of essential services or digital service providers under the NIS Regulations or this Act."

Member's explanatory statement
This amendment would require the Government to consult on establishing data minimisation and anonymisation standards for public bodies, with the view of increasing cyber security and resilience.

LORD BIRT
LORD MARKHAM
LORD CLEMENT-JONES
BARONESS KIDRON

★ After Clause 58, insert the following new Clause—

"Review of the effectiveness of the NIS regime

(1) The Secretary of State must, within 12 months of the day on which this Act is passed, carry out a review of the effectiveness of this Act and the NIS Regulations in securing the security and resilience of the network and information systems on which the economy and the day-to-day functioning of society in the United Kingdom depend.

(2) In particular, the review must, in the context of the regulatory system established by this Act and the NIS Regulations—
   (a) identify the categories of organisation, in both the public and private sectors, that have a material impact on the economy, society or national defence and security, and identify what obligations could be placed upon them to improve their cyber resilience,
   (b) review the critical vulnerabilities of technology platforms and identify what obligations could be placed on technology providers to supply safe services, and to address vulnerabilities when they occur, and
   (c) review the options for regulating organisations and technology providers to promote cyber resilience.

(3) The review must consider—
   (a) the sectors and activities currently within scope,
   (b) the management of supply chain risks,

(c) whether further sectors and activities should be specified as essential activities under section 24(3), or otherwise brought within the scope of the NIS Regulations, having particular regard to—

(i) all sectors forming part of the United Kingdom's critical national infrastructure,

(ii) digital infrastructure, including cloud services, software-as-a-service, and content delivery networks,

(iii) frontier artificial intelligence models and systems, or other frontier agentic technologies,

(iv) democratic processes, including election administration and registered political parties,

(v) advanced manufacturing, life sciences, and critical transport equipment, and

(vi) sectors of social importance, including education, research organisations, and large-scale retail distribution of essential goods other than food,

(d) the institutional and regulatory framework established or otherwise affected by this Act and the NIS Regulations, including the roles and powers of the Secretary of State, designated competent authorities, the National Cyber Security Centre, the Information Commissioner, and the AI Security Institute.

(4) In considering the sectors and activities currently within scope, the Secretary of State must assess—

(a) whether essential activities are appropriately defined and effectively regulated,

(b) whether the thresholds for regulation under the NIS Regulations, including those which exclude micro and small enterprises, leave significant risks unaddressed, and

(c) how effectively risks arising in supply chains are managed.

(5) In considering the regulatory system established or otherwise affected by this Act and the NIS Regulations, the Secretary of State must consider—

(a) the institutional framework for the exercise of functions under this Act and the NIS Regulations, including the roles and powers of the Secretary of State, the designated competent authorities, the National Cyber Security Centre and the Information Commission, and whether that framework is the optimum framework for promoting cyber resilience across the United Kingdom,

(b) the obligations to promote cyber resilience placed on—

(i) persons within scope of the NIS Regulations,

(ii) other organisations and sectors which could facilitate or contribute to security or operational compromises of relevant network and information systems,

(iii) the developers of emerging and frontier technologies which could compromise relevant network and information systems, and

(iv) organisations and sectors making a material impact on the economy, society, defence or security of the United Kingdom.

(d) the powers of the AI Security Institute in relation to frontier AI systems that pose a material risk to the security or resilience of network and information systems used in essential activities—

(i) to audit such systems before they are deployed or made available for use in such network and information systems,

(ii) to set and review safety standards for such systems,

(iii) to inspect such systems and the practices of their developers and deployers, and

(iv) to require remedial action, including the suspension or restriction of the provision or deployment of a system, or to recommend that the Secretary of State do so,

(e) whether the supply of cyber security professionals required to ensure security or resilience of network and information systems used in essential activities is sufficient, and

(f) the obligations placed on regulated persons to report notifications of incidents, including whether the timelines and notifications are sufficient.

(6) In carrying out the review, the Secretary of State must have regard to—

(a) the impact that an incident affecting network and information systems relied on in the carrying on of an activity would be likely to have on the economy or the day-to-day functioning of society in the United Kingdom or any part of it,

(b) the role of persons carrying on the activity in the supply of essential goods and services and in supply chains,

(c) the extent to which the activity is already subject to comparable requirements relating to the security and resilience of network and information systems, and

(d) the need for regulation to be proportionate, evidence-based and transparent.

(7) In carrying out the review, the Secretary of State must consult—

(a) the National Cyber Security Centre,

(b) the Information Commission,

(c) the designated competent authorities,

(d) the AI Security Institute, and

(e) such other persons as the Secretary of State considers appropriate.

(8) On completing the review, the Secretary of State must lay before Parliament a report setting out—

(a) the findings of the review on each of the matters mentioned in subsections (2) and (3),

(b) the activities (if any) which the Secretary of State intends to specify as essential activities, or otherwise to bring within the scope of the NIS Regulations, and the timetable for doing so,

(c) the reasons for not bringing within scope any activity mentioned in subsection (4) or (5) which the Secretary of State does not intend to bring within scope, and

(d) the changes (if any) which the Secretary of State intends to make to the regulatory system, and the timetable for doing so.

(9) Where a report under subsection (10) concludes that an activity should be brought within the scope of the NIS Regulations or of regulations under section 29(1), the Secretary of State must, within six months of the report being laid—

(a) lay before Parliament a draft of regulations under section 24(3) specifying that activity, or

(b) lay before Parliament a statement explaining why the Secretary of State does not intend to do so.

(10) The Secretary of State must, at intervals of not more than 12 months after the report under subsection (8) is laid, carry out a further review in accordance with subsections (1) to (8) and lay before Parliament a report on that review setting out the matters mentioned in subsection (10).

(11) In this section—

"frontier AI system" means a highly capable general-purpose artificial intelligence model or system that can perform a wide variety of tasks and matches or exceeds the capabilities of the most advanced contemporary models;

"frontier agentic technology" means any machine-based system which, for explicit or implicit objectives, infers from the input it receives how to generate outputs that can influence physical or virtual environments, and which—

(a) can act autonomously, taking sequences of actions without human direction, and can adaptably achieve complex goals in complex environments with limited direct human supervision, and

(b) has capabilities which match or exceed those present in the most advanced AI models or systems at the time."

Member's explanatory statement

This amendment would require the Secretary of State to review, within 12 months, the effectiveness of the Act and the NIS Regulations, including on sectors within scope and the regulatory framework under which the NIS Regulations operate, and the obligations that could be placed on organisations and technology providers to improve their cyber resilience.

Clause 60

VISCOUNT CAMROSE
LORD MARKHAM

Clause 60, page 86, line 2, leave out subsections (1) and (2) and insert—

(1) Section (*Publication of relevant elements of the National Cyber Action Plan*) and this Part come into force on the day on which this Act is passed.

(2) The other provisions of this Act may not come into force in accordance with subsection (3) until the requirements set out in section (*Publication of relevant elements of the National Cyber Action Plan*) have been met."

Member's explanatory statement
This amendment, and another in the name of Viscount Camrose, makes commencement of the rest of the Act conditional on publication of relevant elements of the Government's National Cyber Action Plan.

LORD CLEMENT-JONES

★ Clause 60, page 86, line 19, at end insert—

"(5A) Regulations under subsection (3) may not bring section 43 into force unless the following provisions are in force, or are brought into force by the same regulations on or before the day on which section 43 comes into force—

(a) section (*Supplier-related directions: safeguards*),
(b) section (*Supplier-related directions: notice and representations*),
(c) section (*Supplier-related directions: judicial authorisation*),
(d) section (*Supplier-related directions: review, renewal and remedies*),
(e) section (*Supplier-related directions: oversight and proceedings*), and
(f) section (*Supplier-related directions: annual report*)."

Member's explanatory statement
This amendment would ensure that the statutory safeguards, judicial oversight and reporting provisions relating to supplier-related directions are brought into force no later than the commencement of the direction-making powers under section 43.

Cyber Security and Resilience (Network and Information Systems) Bill

RUNNING LIST OF ALL

AMENDMENTS ON REPORT

Tabled up to and including

20 October 2026

20 October 2026

PUBLISHED BY AUTHORITY OF THE HOUSE OF LORDS