

Cyber Security and Resilience (Network and Information Systems) Bill

RUNNING LIST OF ALL AMENDMENTS IN GRAND COMMITTEE

*Tabled up to and including
26 August 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 “on the Secretary of State”

Member's explanatory statement

This amendment is consequential on my new new Clause (Functions under this Part).

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 4

BARONESS KIDRON

Clause 4, page 3, line 18, at end insert –

- “(3A) A data centre also meets the threshold requirement in this paragraph, regardless of its rated IT load, if the Office of Communications considers that an incident affecting the data centre would be likely to have a significant impact on the economy or the day-to-day functioning of society in the United Kingdom or any part of it, having regard in particular to the data centre’s customer base and level of interconnection with essential services.”

Member's explanatory statement

The amendment seeks to add a risk-based designation criterion alongside the existing megawatt thresholds for operators of essential services.

Clause 6

BARONESS LLOYD OF EFFRA

Clause 6, page 4, line 31, after “controller” insert “ –

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

Member's explanatory statement

This amendment would ensure that the threshold requirement relating to the essential service of load control, inserted by Clause 6 of the Bill, applies only to organisations which carry out activities for system-balancing purposes.

BARONESS LLOYD OF EFFRA

Clause 6, page 5, line 5, at end insert –

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

Member's explanatory statement

This amendment would set out when an activity is carried on for “system-balancing purposes” for the purposes of my other amendment to Clause 6.

Clause 7BARONESS KIDRON
LORD CLEMENT-JONES

Clause 7, page 6, line 31, after “engine” insert “, an AI product or service”

Member's explanatory statement

This amendment probes whether the definition of “relevant digital service” being inserted into the NIS Regulations by this bill includes generative-AI models, including but not limited to AI agents and large language models.

LORD BIRT
LORD LONDESBOROUGH

Clause 7, page 6, line 31, after “engine” insert “, software or a digital platform,”

Member's explanatory statement

This amendment, and others in the name of Lord Birt, seek to include software and platform providers in the definition of a relevant digital service provider.

BARONESS KIDRON

Clause 7, page 7, line 23, after “2003/361/EC” insert “, unless the Information Commission or Artificial Intelligence Security Institute determines that the person’s provision of the relevant digital service poses a risk to public safety, national security, or the security of network and information systems relied on for the carrying on of essential activities that is disproportionate to the size of the person”

Member's explanatory statement

This amendment seeks to designate a “relevant digital service provider” under the size-threshold if it provides services which, if disrupted, would cause significant harm to essential activities, public safety, or national security, irrespective of size.

LORD BIRT
LORD LONDESBOROUGH

Clause 7, page 7, line 28, after “nature;” insert —

“and in the case of software or a digital platform, includes a person which—

- (i) creates software for distribution,
- (ii) distributes software on behalf of other businesses,
- (iii) manages services for the distribution of software, or
- (iv) supports software on behalf of others.”

Member's explanatory statement

This amendment, and others in the name of Lord Birt, seek to include software and platform providers in the definition of a relevant digital service provider.

Clause 8

BARONESS LUDFORD
LORD CLEMENT-JONES

Clause 8, page 7, line 36, at end insert –

“(1A) In paragraph (1), after “risks” insert “, including risks arising from fraud,”.”

Member's explanatory statement

This amendment would explicitly include risks arising from fraud as one of the risks to the security of network and information systems that relevant digital service providers must identify and manage.

LORD BIRT
LORD LONDESBOROUGH

Clause 8, page 7, line 36, at end insert –

“(1A) In paragraph (1), after “engine;” insert –

“(ba) software or a digital platform;”.”

Member's explanatory statement

This amendment, and others in the name of Lord Birt, seek to include software and platform providers in the definition of a relevant digital service provider.

LORD TARASSENKO

Clause 8, page 8, line 7, leave out from “Commission” to end of line 8 and insert “and the Artificial Intelligence Security Institute when carrying out the duties imposed on it by paragraph (1) of the NIS Regulations when they rely on an AI product or service within the UK.”

Member's explanatory statement

This amendment seeks to require RSDPs to follow guidance issued by the ICO and AISI when identifying and taking proportionate measures to manage the risks posed to the security of network and information systems which it relies on to provide services within the UK.

Clause 9

BARONESS KIDRON

Clause 9, page 8, line 24, after “2003/361/EC” insert “, unless the Information Commission determines that the person’s provision of the relevant service poses a risk to public safety, national security, or the security of network and information systems relied on for the carrying on of essential activities that is disproportionate to the size of the person”

Member's explanatory statement

This amendment seeks to designate a relevant managed service provider under the size-threshold if it provides services which, if disrupted, would cause significant harm to essential activities, public safety, or national security.

LORD CLEMENT-JONES

Clause 9, page 9, line 13, 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 26, at end insert –

“Restrictions on designation: systemic risk

14IA. – (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.”

Member's explanatory statement

This amendment establishes a statutory distinction between single-entity and systemic risk, ensuring that the "critical supplier" designation is strictly reserved for entities presenting genuine multi-sectoral or macro-economic risks. It also mandates cross-sectoral statutory guidance to ensure consistency across all 12 sectoral regulators.

Clause 15

BARONESS NEVILLE-JONES

Clause 15, page 21, line 19, leave out “capable of having” and insert “likely to have”

Member's explanatory statement

This amendment would narrow the definition of “incident” in regulation 1(2) of the NIS Regulations so that it covers events likely to have an adverse effect, rather than events capable of having one, aligning the definition with the likelihood tests applied to notification later in the Bill.

BARONESS HARDING OF WINSCOMBE

Clause 15, page 21, line 33, at end insert –

- “(c) if requested by the designated competent authority following the full notification, an intermediate report containing such information on the status of the incident, and updating the information given under paragraph (2)(b), as the authority may specify, and
- (d) a final report containing the information listed in paragraph (5A) in relation to the incident.”

BARONESS LLOYD OF EFFRA

Clause 15, page 22, line 14, leave out “users of”

Member's explanatory statement

This amendment would require an operator of an essential service to consider whether any data relating to the essential service has been compromised (not just data relating to users of the service) when determining whether an incident should be reported.

BARONESS HARDING OF WINSCOMBE

Clause 15, page 22, line 15, 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.”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 22, line 28, at end insert –

- “(5A) The information referred to in paragraph (2)(d) is –
 - (a) a detailed description of the incident, including its severity and impact;
 - (b) the type of threat or root cause which is likely to have caused the incident;
 - (c) the mitigation measures applied and, so far as known to the OES, ongoing;
 - (d) so far as known to the OES, any cross-border impact of the incident.”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 22, line 30, after “notification,” insert “without undue delay and in any event”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 22, line 33, after “notification,” insert “without undue delay and in any event”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 22, line 34, at end insert –

- “(c) in the case of an intermediate report, before the end of such period as the designated competent authority may specify when requesting the report, being a period of not more than 14 days beginning with the date of the request.
- (d) In the case of a final report, no later than the end of the period of one month beginning with the time at which the full notification is given.”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 22, line 34, at end insert –

- “(6A) Where the OES incident is still occurring at the time a final report would otherwise fall to be given under paragraph (6)(d), the OES must instead give –
 - (a) a progress report, at the time provided for in paragraph (6)(d), containing the information listed in paragraph (5A) so far as then known; and

- (b) a final report, containing the information listed in paragraph (5A), before the end of the period of one month beginning with the time at which the OES incident ceases.”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 23, line 12, at end insert –

- “(c) if requested by the designated competent authority following the full notification, an intermediate report containing such information on the status of the incident, and updating the information given under paragraph (2)(b), as the authority may specify, and
- (d) a final report containing the information listed in paragraph (4A) in relation to the incident.”

BARONESS NEVILLE-JONES

Clause 15, page 23, line 13, leave out “could have had”

Member's explanatory statement

This amendment would remove the reference to an incident which could have had an impact from the definition of “data centre incident”, so that the definition covers incidents which have had, are having or are likely to have a significant impact.

BARONESS HARDING OF WINSCOMBE

Clause 15, page 23, line 35, at end insert –

- “(4A) The information referred to in paragraph (2)(d) is –
- (a) a detailed description of the incident, including its severity and impact;
- (b) the type of threat or root cause which is likely to have caused the incident;
- (c) the mitigation measures applied and, so far as known to the OES, ongoing;
- (d) so far as known to the OES, any cross-border impact of the incident.”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 23, line 37, after “notification” insert “without undue delay and in any event”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 23, line 40, after “notification” insert “without undue delay and in any event”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 23, line 41, at end insert –

- “(c) in the case of an intermediate report, before the end of such period as the designated competent authority may specify when requesting the report, being a period of not more than 14 days beginning with the date of the request.
- (d) In the case of a final report, no later than the end of the period of one month beginning with the time at which the full notification is given.”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 23, line 41, at end insert –

- “(5A) Where the data centre incident is still occurring at the time a final report would otherwise fall to be given under paragraph (5)(d), the OES must instead give –
 - (a) a progress report, at the time provided for in paragraph (5)(d), containing the information listed in paragraph (4A) so far as then known; and
 - (b) a final report, containing the information listed in paragraph (4A), before the end of the period of one month beginning with the time at which the data centre incident ceases.”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 26, line 12, at end insert –

- “(c) if requested by the Information Commission or Artificial Intelligence Security Institute following the full notification, an intermediate report containing such information on the status of the incident, and updating the information given under paragraph (1)(b), as the Information Commission may specify, and
- (d) a final report containing the information listed in paragraph (4A) in relation to the incident.”

BARONESS LLOYD OF EFFRA

Clause 15, page 26, line 31, leave out “users of”

Member's explanatory statement

This amendment would require a relevant digital service provider to consider whether any data relating to the relevant digital service has been compromised (not just data relating to users of the service) when determining whether an incident should be reported.

BARONESS HARDING OF WINSCOMBE

Clause 15, page 27, line 10, at end insert –

- “(4A) The information referred to in paragraph (1)(d) is –

- (a) a detailed description of the incident, including its severity and impact;
- (b) the type of threat or root cause which is likely to have caused the incident;
- (c) the mitigation measures applied and, so far as known to the RDSP, ongoing;
- (d) so far as known to the RDSP, any cross-border impact of the incident.”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 27, line 12, after “notification” insert “without undue delay and in any event”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 27, line 15, after “notification” insert “without undue delay and in any event”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 27, line 16, at end insert —

- “(c) in the case of an intermediate report, before the end of such period as the designated competent authority may specify when requesting the report, being a period of not more than 14 days beginning with the date of the request.
- (d) In the case of a final report, no later than the end of the period of one month beginning with the time at which the full notification is given.”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 27, line 16, at end insert —

- “(5A) Where the RDSP incident is still occurring at the time a final report would otherwise fall to be given under paragraph (5)(d), the RDSP must instead give —
 - (a) a progress report, at the time provided for in paragraph (5)(d), containing the information listed in paragraph (4A) so far as then known; and
 - (b) a final report, containing the information listed in paragraph (4A), before the end of the period of one month beginning with the time at which the RDSP incident ceases.”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 29, line 24, at end insert —

- “(c) if requested by the Information Commission following the full notification, an intermediate report containing such information on the status of the incident, and updating the information given under paragraph (1)(b), as the Information Commission may specify, and
- (d) a final report containing the information listed in paragraph (4A) in relation to the incident.”

BARONESS LLOYD OF EFFRA

Clause 15, page 30, line 4, leave out “users of”

Member's explanatory statement

This amendment would require a relevant managed service provider to consider whether any data relating to the relevant managed service has been compromised (not just data relating to users of the service) when determining whether an incident should be reported.

BARONESS HARDING OF WINSCOMBE

Clause 15, page 30, line 24, at end insert –

“(4A) The information referred to in paragraph (1)(d) is –

- (a) a detailed description of the incident, including its severity and impact;
- (b) the type of threat or root cause which is likely to have caused the incident;
- (c) the mitigation measures applied and, so far as known to the RMSP, ongoing;
- (d) so far as known to the RMSP, any cross-border impact of the incident.”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 30, line 26, after “notification” insert “without undue delay and in any event”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 30, line 29, after “notification” insert “without undue delay and in any event”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 30, line 30, at end insert –

- “(c) in the case of an intermediate report, before the end of such period as the designated competent authority may specify when requesting the report, being a period of not more than 14 days beginning with the date of the request.
- (d) In the case of a final report, no later than the end of the period of one month beginning with the time at which the full notification is given.”

BARONESS HARDING OF WINSCOMBE

Clause 15, page 30, line 30, at end insert –

“(5A) Where the RMSP incident is still occurring at the time a final report would otherwise fall to be given under paragraph (5)(d), the RMSP must instead give –

- (a) a progress report, at the time provided for in paragraph (5)(d), containing the information listed in paragraph (4A) so far as then known; and
- (b) a final report, containing the information listed in paragraph (4A), before the end of the period of one month beginning with the time at which the RMSP incident ceases.”

Clause 16

BARONESS HARDING OF WINSCOMBE

Clause 16, page 32, line 34, leave out “as soon as reasonably practicable” and insert “without delay and in any event within 24 hours of becoming aware of the incident”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 32, line 36, leave out “adversely”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 33, line 1, leave out “adversely”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 33, line 6, at end insert —

- “(ba) if the incident has caused or is capable of causing severe operational disruption of the services or financial loss for the customer concerned,
- (bb) if the incident has affected or is capable of affecting related natural or legal persons to the customer by causing considerable material or non-material damage, and”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 33, line 11, leave out “adversely”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 33, line 11, at end insert —

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

BARONESS HARDING OF WINSCOMBE

Clause 16, page 33, line 15, leave out “as soon as reasonably practicable” and insert “without delay and in any event within 24 hours of becoming aware of the incident”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 33, line 17, leave out “adversely”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 33, line 21, leave out “adversely”

BARONESS HARDING OF WINSCOMBE

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

- “(ba) if the incident has caused or is capable of causing severe operational disruption of the services or financial loss for the customer concerned,
- (bb) if the incident has affected or is capable of affecting related natural or legal persons to the customer by causing considerable material or non-material damage, and”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 33, line 31, leave out “adversely”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 33, line 31, at end insert—

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

BARONESS HARDING OF WINSCOMBE

Clause 16, page 33, line 35, leave out “as soon as reasonably practicable” and insert “without delay and in any event within 24 hours of becoming aware of the incident”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 33, line 37, leave out “adversely”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 34, line 3, leave out “adversely”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 34, line 8, at end insert—

- “(ba) if the incident has caused or is capable of causing severe operational disruption of the services or financial loss for the customer concerned,

- (bb) if the incident has affected or is capable of affecting related natural or legal persons to the customer by causing considerable material or non-material damage, and”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 34, line 13, leave out “adversely”

BARONESS HARDING OF WINSCOMBE

Clause 16, page 34, line 13, at end insert –

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

After Clause 16

BARONESS HARDING OF WINSCOMBE

After Clause 16, insert the following new Clause –

“Notification of near misses, cyber threats and sub-threshold incidents

After regulation 14G of the NIS Regulations insert –

“Notification of near misses, cyber threats and sub-threshold incidents

14GA. – (1) A regulated person must notify the designated competent authority without undue delay and in any event no later than 72 hours of becoming aware, of –

- (a) a cyber threat, or
- (b) a near miss,
- (c) a sub-threshold incident affecting the regulated person's network and information systems.

(2) A person other than a regulated person may notify the designated competent authority on a voluntary basis of a significant incident, a cyber threat or a near miss affecting that person's network and information systems, regardless of whether that person is subject to any requirement under these Regulations.

(3) Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, a person who gives a notification under paragraph (1) or (2) is not, by reason only of that notification, subject to any additional duty, liability or requirement to which that person would not otherwise have been subject.

(4) In this regulation –

“cyber threat” means any potential circumstance, event or action that could, if it occurred, adversely affect the network and information systems of a person, or the users of a service provided by means of such systems;

“near miss” means an event that could have compromised the availability, authenticity, integrity or confidentiality of data, or of a service provided by

means of network and information systems, but that was prevented from having that effect or did not in fact have that effect;

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

“sub-threshold incident” means an incident affecting the regulated person's network and information systems which the regulated person is not otherwise required to notify under regulation 11(2), 11A(2), 12A(1) or 14E(1).”

Member's explanatory statement

This new clause seeks to ensure that regulated persons must report to their designated competent authority any near miss incident, cyber threat, or sub-threshold incident that could adversely affect the network and information systems of a person, or the users of a service provided by means of such systems.

Clause 18

LORD ALTON OF LIVERPOOL
LORD HUNT OF KINGS HEATH
LORD MARKHAM
BARONESS LUDFORD

Clause 18, page 41, line 7, at end insert –

“Exemption from disclosure: right to a fair trial

6AA. – (1) Nothing in paragraphs (1)(d) to (f) of regulation 6, or regulation 6A, permits a NIS enforcement authority to share information with another NIS enforcement authority or with a person within paragraph (2) of regulation 6 if the Secretary of State determines that –

- (a) the receiving jurisdiction is one in which the right to a fair trial cannot be guaranteed, or
- (b) the disclosure could result in actions being taken that would be incompatible with the right to a fair trial.

(2) For the purposes of making a determination under paragraph (1) above, the Secretary of State must have regard to the opinion of –

- (a) subject matter experts, and
- (b) competent civil society groups.

(3) Every 12 months the Secretary of State must publish and lay before Parliament an annual report detailing the determinations made under paragraph (1) in the previous 12 months.

(4) The first report under paragraph (3) must be published and laid within 12 months of the day on which the Cyber Security and Resilience (Network and Information Systems) Act 2026 is passed.”

After Clause 21

BARONESS MORGAN OF COTES
BARONESS KIDRON
BARONESS LUDFORD

After Clause 21, insert the following new Clause —

“Liability of senior executives

After regulation 18 of the NIS Regulations insert —

“Liability of senior executives

18A.— (1) This regulation applies where a designated competent authority or the Information Commission has reasonable grounds to believe that —

- (a) a person that is a body corporate, a partnership (including a Scottish partnership) or an unincorporated body has failed to comply with a duty referred to in regulation 17(1), (2), (2ZA) or (2ZB), and
- (b) the failure was committed with the consent or connivance of, or is reasonably attributable to any neglect on the part of, a senior executive or group of senior executives, deliberately or carelessly.

(2) The competent authority or the Information Commission may serve a notice of intention to impose a penalty on the senior executive(s) if it considers that a penalty is warranted having regard to the facts and circumstances of the case.

(3) Before serving a senior executive(s) notice, the authority or the Information Commission must inform the senior executive(s), in such form and manner as it considers appropriate having regard to the facts and circumstances of the case, of —

- (a) the alleged failure and the office’s alleged consent, connivance or neglect, and
- (b) how and by when representations may be made in relation to the alleged failure and any related matters.

(4) A senior executive(s) notice must be in writing and must specify the following —

- (a) the reasons for serving the notice;
- (b) the alleged failure or failures and the senior executive(s) alleged consent, connivance, neglect or carelessness which are the subject of the notice;
- (c) any remedial actions required;
- (d) the amount of the penalty and the number of penalties which the authority or the Information Commission is minded to impose.

(5) The authority or the Information Commission may, after considering any representations made in accordance with paragraph (3)(b), serve a penalty notice on the officer with a final penalty decision if satisfied that a penalty is warranted having regard to the facts and circumstances of the case.

(6) A penalty imposed under this regulation must be of an amount which the authority or the Information Commission determines is appropriate and proportionate in the circumstances, having regard to the matters mentioned in regulation 18(6) for each infringement individually.

(7) If the authority or the Information Commission is satisfied that no further action is required, having considered any representations submitted in accordance with paragraph (3)(b), it must inform the senior executive(s) in writing as soon as reasonably practicable.

(8) In this regulation “senior executive(s)” –

- (a) in relation to a body corporate, means a CEO, director, manager, secretary or other similar senior executive of the body, or a person purporting to act in any such capacity;
- (b) in relation to a partnership, means a partner or a person having control or management of the partnership business, or a person purporting to act in any such capacity;
- (c) in relation to an unincorporated body other than a partnership, means a member of its governing body, or a person purporting to act in any such capacity.””

Member's explanatory statement

This amendment seeks to create provision in the Bill for executives or senior managers to be held responsible for failure to comply or report on the measures placed upon regulated bodies within the Bill.

After Clause 23

BARONESS KIDRON
LORD CLEMENT-JONES
BARONESS HARDING OF WINSCOMBE

After Clause 23, insert the following new Clause –

“Red lines on AI products and services

- (1) AI products and services which are classified as “relevant digital services” for the purposes of the NIS Regulations must demonstrate they are not capable of performing capabilities that cross “red lines” as defined in subsection (2).
- (2) The red lines referred to in subsection (1) are –
 - (a) evading human oversight or shutdown or resisting any action that, at a given level of confidence, compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, network and information systems,
 - (b) autonomously self-replicating, self-improving, or acquiring compute or other resources to the extent that this presents a risk to the authenticity and integrity of the processed data held within the system,

- (c) autonomously conducting or substantially accelerating sophisticated attacks on critical infrastructure, including government, security, services, policing, health services, education services, banking and finance, public utilities, food and water, and any other relevant network and information system,
 - (d) providing support for the development of chemical, biological, radiological, or nuclear weapons by non-state actors or hostile states to facilitate attacks on critical infrastructure, including government, security services, policing, health services, education services, banking and finance, public utilities, food and water, and any other relevant network and information system,
 - (e) providing support for terrorist groups and hostile actors to facilitate attacks on critical infrastructure, including government, security services, policing, health services, education services, banking and finance, public utilities, food and water, and any other relevant network and information system,
 - (f) deceiving or manipulating populations at scale or compromising confidence in a network and information system's ability to resist any action that compromises the availability, authenticity, integrity or confidentiality of the services offered by those systems,
 - (g) other capabilities which are found to compromise, at a given level of confidence, the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.
- (3) In order to demonstrate successfully that the product or service is not capable of performing capabilities that cross the "red lines" as defined in subsection (2) the AI product or service classified as a "relevant digital service" for the purposes of the NIS Regulations must be assessed and approved by the Artificial Intelligence Security Institute before it is made available within the United Kingdom.
- (4) In this section, "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 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 24

LORD BIRT
LORD LONDESBOROUGH
LORD CLEMENT-JONES

Clause 24, page 51, line 15, at end insert —

“(3A) In specifying an activity for the purposes of subsection (3), the Secretary of State must consider any recommendations they receive from the Office for Cyber Resilience.”

Member's explanatory statement

This amendment seeks to ensure that the Secretary of State considers Office for Cyber Resilience recommendations for essential activities.

LORD BIRT
LORD LONDESBOROUGH

Clause 24, page 51, line 17, leave out from “essential” to end of line 22 and insert “because it has —

- (a) a material economic impact,
- (b) a material societal impact, or
- (c) an impact on national security or defence.”

Member's explanatory statement

This amendment seeks to allow an activity to be specified as essential if it has a material economic or societal impact, or affects national security or defence.

BARONESS LLOYD OF EFFRA

Clause 24, page 51, 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 is a technical amendment and would ensure all essential services in the NIS Regulations are captured.

After Clause 24

BARONESS LUDFORD

After Clause 24, insert the following new Clause —

“Services to support political parties to be specified as essential activities

- (1) The Secretary of State must, within six months of the day on which this Act is passed, make regulations under section 24(3) to specify that an activity carried out for the primary purpose of the operation of a registered political party be an essential activity.
- (2) In this section “registered political party” means a party registered under Part 2 of the Political Parties, Elections and Referendums Act 2000.
- (3) Regulations made under subsection (1) must designate one or more appropriate regulatory authorities for the specified activities.”

Member's explanatory statement

This new clause would require the Secretary of State to specify services with the primary aim to support the operation of political parties as essential activities under Part 3, bringing them within the scope of the Bill's security and resilience regime.

BARONESS NORTHOVER
BARONESS HARDING OF WINSCOMBE

After Clause 24, insert the following new Clause —

“Critical manufacturing and retail to be specified as essential activities

- (1) The Secretary of State must, within six months of the day on which this Act is passed, make regulations under section 24(3) to specify the following as essential activities —
 - (a) the manufacture of critical transport equipment, including the manufacture of vehicles,
 - (b) the industrial production and processing of food products, and
 - (c) the retail sale of food and essential goods through large-scale distribution chains.
- (2) Regulations made under subsection (1) must designate one or more appropriate regulatory authorities for the activities so specified.”

Member's explanatory statement

This new clause would require the Secretary of State to specify vehicle and other critical transport-equipment manufacturing, industrial food production, and large-scale food and essential-goods retail distribution as essential activities under Part 3, bringing them within the scope of the Bill's security and resilience regime.

BARONESS NORTHOVER

After Clause 24, insert the following new Clause —

“Space sector to be specified as an essential activity

- (1) The Secretary of State must, within six months of the day on which this Act is passed, make regulations under section 24(3) to specify activities carried on in the space sector as essential activities.
- (2) Regulations made under subsection (1) must designate one or more appropriate regulatory authorities for the space sector.
- (3) In this section, “the space sector” means the sector identified as the space sector in the Government’s Industrial Strategy, and includes —
 - (a) the manufacture of satellites, launch vehicles and ground systems,
 - (b) the provision of launch and in-orbit services,
 - (c) the operation of satellites and satellite constellations, and
 - (d) the provision of satellite-based services, including position, navigation and timing services and satellite communications.”

Member's explanatory statement

This new clause would require the Secretary of State to specify the space sector, as identified in the Government’s Industrial Strategy, as an essential activity under Part 3, bringing space operators within the scope of the Bill’s regime.

Clause 25

LORD RAVENSDALE

Clause 25, page 52, line 20, at end insert —

- “(2A) In preparing a statement under this section, the Secretary of State must have regard to any timelines published by the National Cyber Security Centre for the migration of network and information systems to post-quantum cryptography.”

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.

After Clause 28

BARONESS KIDRON

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,
 - (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.

After Clause 29

LORD CLEMENT-JONES
BARONESS KIDRON
BARONESS HARDING OF WINSCOMBE

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.
- (1A) 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 service;
 - “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 directions 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 (6) 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 (7)(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 (9) 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 centers, in the event of an AI security or operational emergency.

After Clause 35

LORD CLEMENT-JONES

After Clause 35, insert the following new Clause –

“Office for Cyber Resilience (No. 1)

- (1) There is to be a body corporate known as the Office for Cyber Resilience (“the OCR”).
- (2) The OCR is to be –
 - (a) the single regulatory authority for the purposes of this Act, and
 - (b) the single designated competent authority for the purposes of the NIS Regulations.
- (3) The Secretary of State must by regulations –
 - (a) provide for the transfer to the OCR of the functions of –
 - (i) each designated competent authority under the NIS Regulations, and
 - (ii) each regulatory authority designated under Chapter 1 of this Part,
 - (b) make provision for the OCR to exercise those functions in place of the authorities mentioned in paragraph (a), and
 - (c) make such transitional, transitory, saving, consequential and supplementary provision as the Secretary of State considers appropriate in connection with the establishment of the OCR, including provision amending this Act, the NIS Regulations or any other enactment.
- (4) Regulations under subsection (3) must in particular make provision about the OCR’s constitution, membership, staffing, funding, governance and accountability to Parliament.
- (5) In exercising its functions the OCR must –
 - (a) act in a way that is proportionate, consistent, transparent and targeted only at cases in which action is needed,
 - (b) have regard to differences in the nature, scale and risk profile of the sectors and persons it regulates, and
 - (c) maintain arrangements for co-operation with the National Cyber Security Centre, the Information Commission and other relevant persons.
- (6) The Secretary of State must, before the OCR assumes any function, lay before Parliament a report setting out –
 - (a) how the OCR will be resourced and staffed to discharge its functions across all regulated sectors, and
 - (b) the arrangements for maintaining sector-specific technical expertise within the OCR.”

Member's explanatory statement

This new clause seeks to replace the Bill’s current model of multiple sectoral regulators with a single, overarching regulator, the Office for Cyber Resilience. It requires the transfer of existing

regulatory functions to the new regulator and a report to Parliament on its resourcing and technical expertise before the new regulator assumes any function.

LORD BIRT
LORD LONDESBOROUGH
LORD CLEMENT-JONES

After Clause 35, insert the following new Clause —

“Office for Cyber Resilience (No. 2)

- (1) Within 12 months of the day on which this Act is passed, the Secretary of State must establish the Office for Cyber Resilience (OCR).
- (2) The OCR is to be —
 - (a) the single regulatory authority for the purposes of this Act,
 - (b) the single designated competent authority for the purposes of the NIS Regulations, and
 - (c) the NIS enforcement authority, including for the purposes of imposing penalties on relevant bodies under regulation 18 of those Regulations.
- (3) The functions and powers of the OCR are to —
 - (a) ensure that the security and resilience of the network and information systems of relevant bodies is effective and audited;
 - (b) define and update security and resilience standards for network and information systems of relevant bodies, including for responding to incidents and for business continuity planning;
 - (c) require relevant bodies to adjust to threats to network and information systems from new and emerging technologies;
 - (d) impose fines on relevant bodies in serious breach of their obligations under the NIS Regulations in line with regulation 18 (penalties);
 - (e) share knowledge of threats and work in partnership with the National Cyber Security Centre;
 - (f) recommend to the Secretary of State activities to be specified as an “essential activity”.
- (4) In this section “relevant body” 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.
- (5) The Secretary of State must by regulations —
 - (a) provide for the transfer to the OCR of the functions of —
 - (i) each designated competent authority under the NIS Regulations, and
 - (ii) each regulatory authority designated under Chapter 1 of this Part,

- (b) make provision for the OCR to exercise those functions in place of the authorities mentioned in paragraph (a), and
- (c) make such transitional, transitory, saving, consequential and supplementary provision as the Secretary of State considers appropriate in connection with the establishment of the OCR, including provision amending this Act, the NIS Regulations or any other enactment.”

LORD BIRT
LORD LONDESBOROUGH
LORD CLEMENT-JONES

After Clause 35, insert the following new Clause –

“Office for Cyber Resilience: software and platform providers

- (1) The OCR must establish and maintain a register of software and platform providers permitted to supply network and information system services as a relevant digital service provider in the United Kingdom to operators of essential services.
- (2) The OCR must require registered software and platform providers –
 - (a) to certify their products as safe when used as directed, and
 - (b) to inform the OCR and all affected customers within 24 hours of the discovery of a new vulnerability or breach affecting network or information services.
- (3) The OCR must not include in its register any software or platform providers which also supply cyber resilience audit services.”

Member's explanatory statement

This amendment seeks to establish a register of software and platform providers permitted to supply services to operators of essential services in the UK and to certify their products as safe for use.

LORD BIRT
LORD LONDESBOROUGH
LORD CLEMENT-JONES

After Clause 35, insert the following new Clause –

“Office for Cyber Resilience: cyber resilience professionals

- (1) The OCR must work with the UK Cyber Security Council to –
 - (a) ensure that relevant bodies have sufficient and appropriately qualified cyber security professionals, and
 - (b) produce a timetable to increase the number of chartered cyber security professionals available to work on the security and resilience of network and information systems of relevant bodies.
- (2) In this section “relevant bodies” 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.”

Member's explanatory statement

This amendment seeks to ensure that the OCR works with the UK Cyber Security Council to ensure that relevant bodies have sufficient and appropriately qualified cyber security professionals.

LORD BIRT
LORD LONDESBOROUGH
LORD CLEMENT-JONES

After Clause 35, insert the following new Clause –

“Office for Cyber Resilience: cyber resilience audit

- (1) Within two years of the day of the establishment of the OCR, and every 12 months thereafter, the OCR must designate which commercial companies and public sector bodies must, from that year on, conduct an annual independent audit of the cyber security and resilience of their network and information systems (“the cyber resilience audit”).
- (2) The OCR may designate those companies or bodies individually or with reference to any relevant categorisation (including sector, scale, or materiality).
- (3) Organisations designated under subsection (1) must be –
 - (a) relevant bodies with respect to the NIS Regulations, or
 - (b) regulated persons within the meaning of this Chapter.
- (4) 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.
- (5) The results of the annual cyber resilience audit must be shared only with the company’s or body’s board, except where any material vulnerabilities or breaches are identified, which must be shared in confidence with the OCR.”

Member's explanatory statement

This amendment seeks to require the Office for Cyber Resilience to designate commercial companies and public sector bodies regulated under the NIS Regulations or the Bill which must conduct an annual independent audit of the cyber security and resilience of their network and information systems.

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.

After Clause 37

LORD CLEMENT-JONES

After Clause 37, insert the following new Clause —

“Consultation before issue of codes of practice and regulations

- (1) Before preparing, issuing, amending or revising a code of practice under this Chapter, the Secretary of State must carry out an open public consultation.
- (2) Before making regulations under section 24 or Chapter 3 of this Part, or giving a direction under Part 4 that applies to a description of regulated persons generally, the Secretary of State must carry out an open public consultation.
- (3) A consultation under this section must —
 - (a) be open to any person providing, or proposing to provide, services of a kind regulated under this Act or the NIS Regulations, and to any other interested person,
 - (b) be published in a manner that is readily accessible, including to small and medium-sized enterprises,
 - (c) last for a period of not less than eight weeks, except where the Secretary of State reasonably considers that a shorter period is justified by urgency and publishes the reasons for that decision, and
 - (d) invite representations on the likely costs, benefits and practical effects of the proposal.
- (4) The Secretary of State must publish a response to the consultation, setting out how the representations received have been taken into account, before the code of practice, regulations or direction take effect.
- (5) This section does not apply to a direction given under Part 4 in respect of a specific regulated person for national security purposes.”

Member's explanatory statement

This new clause would require an open, publicly accessible consultation before the Secretary of State issues or revises codes of practice, makes regulations, or gives directions of general application, and would require publication of a response before they take effect.

After Clause 39

LORD CLEMENT-JONES

After Clause 39, insert the following new Clause —

“Presumption of conformity with recognised standards

- (1) A regulated person who demonstrates compliance with a designated standard in relation to a matter is to be presumed, in relation to that matter, to have complied with the corresponding duty under this Act or the NIS Regulations to which the designated standard relates.

- (2) The Secretary of State must by regulations designate for the purposes of subsection (1) one or more internationally or nationally recognised cyber security standards or frameworks, which must include –
 - (a) the standard published as ISO/IEC 27001 (information security management systems), and
 - (b) the Cyber Essentials Plus certification scheme operated under the authority of the National Cyber Security Centre.
- (3) When designating a standard the Secretary of State must specify the duty or duties under this Act or the NIS Regulations to which the presumption in subsection (1) applies.
- (4) The presumption in subsection (1) –
 - (a) applies only to the extent that the scope of the designated standard covers the network and information systems to which the duty relates, and
 - (b) may be rebutted by a regulatory authority where it has reasonable grounds to believe that, despite compliance with the designated standard, the regulated person has not met the duty in question.
- (5) The Secretary of State must review the designated standards at least once in every three-year period and update them to reflect current best practice.”

Member's explanatory statement

This new clause would create a statutory presumption of conformity so that organisations complying with recognised gold-standard frameworks such as ISO/IEC 27001 or Cyber Essentials Plus are presumed to meet the corresponding security duties, while allowing a regulator to rebut that presumption in an individual case.

Clause 40

LORD CLEMENT-JONES

Clause 40, page 63, line 27, leave out “5” and insert “3”

Member's explanatory statement

This amendment would reduce the maximum interval between the Secretary of State’s reports on the operation of the legislation from five years to three years.

Clause 42

LORD CLEMENT-JONES

Clause 42, page 65, line 36, at end insert –

“(aa) which is made under section (Office for Cyber Resilience), or”

LORD CLEMENT-JONES

Clause 42, page 65, line 36, at end –

“(aa) which is made under section (*Presumption of conformity with recognised standards*), or”

LORD CLEMENT-JONES

★ Clause 42, page 65, line 36, at end insert –

“(aa) which is made under section (*AI Security Institute: standards, inspection and enforcement powers*), or”

After Clause 42

BARONESS NORTHOVER

After Clause 42, insert the following new Clause –

“Cyber security competence: functions of the UK Cyber Security Council

- (1) The UK Cyber Security Council is to exercise the functions described in subsection (2) and is accountable to the Secretary of State for the exercise of those functions.
- (2) The functions are –
 - (a) to validate and accredit professional qualifications, standards and titles for cyber security professionals employed by regulated persons,
 - (b) to monitor the supply of, and demand for, qualified cyber security professionals across the sectors regulated under this Act and the NIS Regulations, and
 - (c) to audit whether, and to what extent, regulated persons employ or have access to appropriately certified cyber security professionals.
- (3) For the purposes of this section, “regulated person” has the same meaning as in Chapter 3 (see section 30).
- (4) A regulatory authority (as defined in section 24) must have regard to the information and standards provided by the Council under this section when exercising its functions.
- (5) The Secretary of State must by regulations made by statutory instrument make further provision about the exercise of the Council’s functions under this section, including provision about its accountability for the exercise of the functions described in subsection (2).
- (6) A statutory instrument containing regulations under this section may not be made unless a draft of the instrument has been laid before and approved by a resolution of each House of Parliament.”

Member's explanatory statement

This new clause would give the UK Cyber Security Council statutory functions to validate qualifications, to monitor the supply of and demand for cyber security professionals in the areas covered by the Bill, and to audit whether regulated organisations employ certified professionals – a “competence mandate” for the regime.

BARONESS NORTHOVER

After Clause 42, insert the following new Clause –

“National cyber security support service for small and medium-sized enterprises

- (1) The Secretary of State must, by regulations, make provision for the establishment and operation of a national cyber security support and incident response service for relevant small and medium-sized enterprises (SMEs), for the purpose of improving the security and resilience of their network and information systems.
- (2) The service established under this section must –
 - (a) be free at the point of use, and
 - (b) provide, in particular following a cyber incident affecting a relevant SME –
 - (i) advice and technical assistance,
 - (ii) incident response support, and
 - (iii) guidance on recovery and remediation.
- (3) For the purposes of this section, a relevant SME is a small or medium-sized enterprise which is –
 - (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) In establishing and operating the service the Secretary of State must have regard to comparable national cyber security support services operated in other jurisdictions.”

Member's explanatory statement

This new clause would require the Secretary of State to establish a national, free-at-the-point-of-use cyber security support and incident response service for relevant SMEs, modelled on comparable overseas services such as the small-business support provided by the Australian Cyber Security Centre.

Before Clause 43

BARONESS LLOYD OF EFFRA

Before Clause 43, insert the following new Clause —

“CHAPTER 1**FUNCTIONS UNDER PART 4****Functions under this Part**

For the purposes of this Part, any reference to the Secretary of State includes a reference to the Chancellor of the Duchy of Lancaster.”

Member's explanatory statement

This amendment would ensure that the functions conferred on the Secretary of State by provisions of Part 4 would also be exercisable by the Chancellor of the Duchy of Lancaster.

BARONESS LLOYD OF EFFRA

Before Clause 43, insert the following new Clause —

“CHAPTER 2**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) in regulations under section 29(1),
 - (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 to national security 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) Where a person is specified in regulations under subsection (1)(a), the appropriate authority must notify the person that they have been so specified.
- (9) For the purposes of subsection (8), the appropriate authority is –
 - (a) where the person is specified in reliance on subsection (2)(a), a regulatory authority in relation to the person;
 - (b) otherwise, the Secretary of State.
- (10) Regulations under subsection (1)(a) may make different provision for different purposes.
- (11) 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 (but see section (*Regulations under section (Vendor-related directions)(1)(a) or 43(1A)(b): procedure in urgent cases*) for further provision about the making of such an instrument in cases of urgency).”

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 to national security 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 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 in regulations under 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 66, 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 66, 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 66, 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 66, 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) in regulations under section 29(1), 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 66, line 8.

BARONESS LLOYD OF EFFRA

Clause 43, page 66, line 16, at end insert “with a view to eliminating, reducing or mitigating the risk to national security 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 66, 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 66, 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 66, 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 66, 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.
- (3B) Where a person is specified in regulations under subsection (1A)(b), the Secretary of State must notify the person that they have been so specified.”

Member's explanatory statement

This amendment is consequential on my amendment to Clause 43 at page 66, line 14, and imposes consultation and notification duties in relation to the regulations.

BARONESS LLOYD OF EFFRA

Clause 43, page 67, 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 67, line 3, 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 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 (but see section *(Regulations under section (Vendor-related directions)(1)(a) or 43(1A)(b): procedure in urgent cases)* for further provision about the making of such an instrument in cases of urgency).”

Member's explanatory statement

This amendment is consequential on my amendment to Clause 43 at page 66, line 14, and would make further provision about the regulations.

Clause 44

BARONESS LLOYD OF EFFRA

Clause 44, page 68, 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 68, 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 68, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 68, 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 68, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 68, line 14, leave out “regulated”

Member's explanatory statement

See the explanatory statement to my amendment to Clause 44 at page 68, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 68, 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 68, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 68, line 24, after “varies the” insert “relevant”

Member's explanatory statement

See the explanatory statement to my amendment to Clause 44 at page 68, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 68, line 26, after “the” insert “relevant”

Member's explanatory statement

See the explanatory statement to my amendment to Clause 44 at page 68, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 68, 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 68, line 4.

BARONESS LLOYD OF EFFRA

Clause 44, page 68, 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 68, line 4.

After Clause 44

BARONESS LLOYD OF EFFRA

After Clause 44, insert the following new Clause —

**“Regulations under section (*Vendor-related directions*)(1)(a) or 43(1A)(b):
procedure in urgent cases**

- (1) A statutory instrument containing regulations under section (*Vendor-related directions*)(1)(a) or 43(1A)(b) may be made without a draft of the instrument being laid before and approved by a resolution of each House of Parliament if it contains a declaration that the Secretary of State considers that, by reason of urgency, it is necessary to make the regulations without a draft being so laid and approved.
- (2) After an instrument is made in accordance with subsection (1), it must be laid before each House of Parliament.
- (3) Regulations contained in an instrument made in accordance with subsection (1) cease to have effect at the end of the period of 28 days beginning with the day on which the instrument is made unless, during that period, the instrument is approved by a resolution of each House of Parliament.
- (4) In calculating the period of 28 days, no account is to be taken of any time during which—
 - (a) Parliament is dissolved or prorogued, or
 - (b) either House of Parliament is adjourned for more than four days.
- (5) If regulations cease to have effect as a result of subsection (3), that does not—
 - (a) affect the validity of anything previously done under the regulations, or
 - (b) prevent the making of new regulations.”

Member's explanatory statement

*This amendment would set out the Parliamentary procedure that would apply to regulations under my new Clause (*Vendor-related directions*) and under Clause 43 in cases of urgency.*

Clause 45

BARONESS LLOYD OF EFFRA

Clause 45, page 68, 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 69, 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 71, 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 71, 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 71, 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 71, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 72, 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 71, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 72, line 3, leave out “regulated” and insert “affected”

Member's explanatory statement

See the explanatory statement to my amendment to Clause 47 at page 71, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 72, 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 71, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 72, 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 71, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 72, line 33, leave out “regulated” and insert “affected”

Member's explanatory statement

See the explanatory statement to my amendment to Clause 47 at page 71, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 72, line 36, leave out “regulated” and insert “affected”

Member's explanatory statement

See the explanatory statement to my amendment to Clause 47 at page 71, line 27.

BARONESS LLOYD OF EFFRA

Clause 47, page 73, line 1, leave out “regulated” and insert “affected”

Member's explanatory statement

See the explanatory statement to my amendment to Clause 47 at page 71, line 27.

Clause 48

BARONESS LLOYD OF EFFRA

Clause 48, page 73, 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 73, 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 75, 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 75, 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 75, 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 75, 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 75, line 18, leave out “regulated”

Member's explanatory statement

This amendment and my amendment to Clause 49 at page 75, line 26 are consequential on my amendments to Clause 47 at page 71, line 33, at page 72, line 1, and at page 72, line 3.

BARONESS LLOYD OF EFFRA

Clause 49, page 75, 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 75, line 8.

BARONESS LLOYD OF EFFRA

Clause 49, page 75, 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 75, line 8.

BARONESS LLOYD OF EFFRA

Clause 49, page 75, line 26, leave out “regulated”

Member's explanatory statement

See the explanatory statement to my amendment to Clause 49 at page 75, line 18.

Clause 52

BARONESS LLOYD OF EFFRA

Clause 52, page 78, 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 80, line 26, after “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 81, 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).

Clause 55

BARONESS LLOYD OF EFFRA

Clause 55, page 81, 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.

Clause 58

BARONESS LLOYD OF EFFRA

Clause 58, page 84, 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 84, line 23).

BARONESS LLOYD OF EFFRA

Clause 58, page 84, 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 84, line 26).

BARONESS LLOYD OF EFFRA

Clause 58, page 84, 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 84, 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 84, 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 84, line 28, after “30(2)” insert “and (5)”

Member's explanatory statement

This is a drafting amendment.

BARONESS LLOYD OF EFFRA

Clause 58, page 84, 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 amendment to Clause 58 at page 84, line 26).

BARONESS LLOYD OF EFFRA

Clause 58, page 84, 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 84, 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, complementing the three-yearly review of the legislation provided for by Lord Clement-Jones' amendment to clause 40.

BARONESS LUDFORD

After Clause 58, insert the following new Clause —

“Digital Sovereignty Strategy

- (1) The Secretary of State must, within 12 months of the day on which this Act is passed, publish a strategy (“the Digital Sovereignty Strategy”) setting out the Government’s approach to maintaining the security and resilience of relevant network and information systems by assessing, managing and mitigating risks —
- (a) associated with foreign interference, and
 - (b) arising from reliance on foreign-supplied technologies.
- (2) The Digital Sovereignty Strategy must —
- (a) include risks associated with —
 - (i) hardware,
 - (ii) software,
 - (iii) supply chains, and
 - (iv) procurement processes;
 - (b) include a specific focus on the security and resilience of government digital procurement, detailing how the Government intends to reduce strategic dependencies on foreign-owned suppliers and on the hardware and software of hostile states so as to mitigate the risk of systemic disruption;
 - (c) include a commitment to prioritise, where appropriate, the use of secure technologies developed in the United Kingdom by United Kingdom organisations in relevant network and information systems;
 - (d) set out how the Government intends to address any risks identified under subsection (1), including by supporting the use of sovereign and domestic technologies or systems.
- (3) The Secretary of State must review and, if necessary, revise the Digital Sovereignty Strategy at least once in every three-year period.
- (4) For the purposes of this section, a “relevant network and information system” is 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 Government to publish, within 12 months, a Digital Sovereignty Strategy addressing risks from foreign interference and reliance on foreign technologies, with a specific focus on reforming government digital procurement to prioritise secure, sovereign and home-grown UK technology.

BARONESS LUDFORD

After Clause 58, insert the following new Clause –

“Board oversight and accountability: security and resilience of network and information systems

- (1) Where a relevant body is governed by a board or equivalent management body, that body must exercise oversight of the arrangements relating to the security and resilience of the body’s network and information systems.
- (2) In exercising that oversight, the management body must –
 - (a) approve the approach taken by the body to the management of risks to the security and resilience of the body’s network and information systems, and
 - (b) satisfy itself, on a periodic basis, that appropriate and proportionate measures are in place to manage those risks.
- (3) The management body may be held accountable for a failure by the body to comply with its duties relating to the security and resilience of its network and information systems.
- (4) Members of the management body must undertake training designed to enable them to identify risks to, and assess appropriate risk-management practices for, the body’s network and information systems.
- (5) For the purposes of this section, a relevant body is one which is –
 - (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 active board-level oversight of, and explicit accountability for, the security and resilience of a relevant body’s network and information systems, including a duty on board members to undertake relevant training, where the body is governed by a board or similar management body.

BARONESS LUDFORD

After Clause 58, insert the following new Clause—

“Review of the regulation of data-storing sectors

- (1) The Secretary of State must carry out a review of whether the NIS Regulations should be extended to persons who store or process personal data on behalf of other organisations at scale, but who are not otherwise regulated under those Regulations.
- (2) The review must, in particular, consider the case for extending regulation to—
 - (a) providers of software as a service,
 - (b) any other sector or description of provider which the Secretary of State considers, at the time of the review, to hold personal data on behalf of other organisations at a scale or in a manner that may warrant regulation under the NIS Regulations.
- (3) In carrying out the review the Secretary of State must consider, in particular—
 - (a) the number of organisations relying on any single such provider, and the number of individuals whose personal data is held;
 - (b) the extent to which those organisations are able in practice to assess or influence the security of the network and information systems on which their data is held;
 - (c) whether the data protection legislation is sufficient to manage the risks identified, in particular as regards the security of network and information systems and the reporting of incidents;
 - (d) whether providers within subsection (2) could be brought within the meaning of “relevant managed service provider” or “relevant digital service provider”, or designated under regulation 14H of the NIS Regulations, and what changes (if any) to those Regulations would be needed to achieve this;
 - (e) the effect of any such extension on organisations that are small or medium-sized enterprises, or that are charities or other voluntary organisations, whether as providers or as customers.
- (4) In carrying out the review the Secretary of State must consult the Information Commission, the National Cyber Security Centre, and such other persons as the Secretary of State considers appropriate.
- (5) The Secretary of State must lay a report on the review before Parliament within 12 months of the day on which this Act is passed.
- (6) In this section—

“the data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);

“the NIS Regulations” has the meaning given by section 1.”

Member's explanatory statement

This probing amendment would require the Secretary of State to review, and report to Parliament within 12 months of Royal Assent, whether cyber security regulation under the NIS Regulations

should be extended to further sectors that store or process personal data on behalf of other organisations at scale, including software-as-a-service providers

Cyber Security and Resilience (Network and Information Systems) Bill

RUNNING LIST OF ALL AMENDMENTS IN GRAND COMMITTEE

*Tabled up to and including
26 August 2026*

26 August 2026

PUBLISHED BY AUTHORITY OF THE HOUSE OF LORDS