Cyber Security and Resilience (Network and Information Systems) Bill

RUNNING LIST OF ALL

AMENDMENTS IN GRAND COMMITTEE

Tabled up to and including

21 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 4

BARONESS KIDRON

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

"(3A) A data centre also meets the threshold requirement in this subsection, 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 7

BARONESS KIDRON

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 large language models and chatbots.

LORD BIRT

★ 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 "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 Regulated 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

★ 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

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

★ 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.

Clause 9

BARONESS KIDRON

★ Clause 9, page 8, line 24, after "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 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 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.

After Clause 21

BARONESS MORGAN OF COTES
BARONESS KIDRON

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

★ 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 attacks conducted by 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

★ 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

★ 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.

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

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.

After Clause 29

LORD CLEMENT-JONES
BARONESS KIDRON

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

(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

★ After Clause 35, insert the following new Clause—

"Office for Cyber Resilience

(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

★ 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

★ 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

★ 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.

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"

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 in described 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.

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.

Cyber Security and Resilience (Network and Information Systems) Bill

RUNNING LIST OF ALL

AMENDMENTS IN GRAND COMMITTEE

Tabled up to and including

21 August 2026

---

21 August 2026

PUBLISHED BY AUTHORITY OF THE HOUSE OF LORDS