Cyber Security and Resilience (Network and Information Systems) Bill

RUNNING LIST OF ALL

AMENDMENTS IN GRAND COMMITTEE

Tabled up to and including

22 July 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 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.

Clause 9

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.

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.

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.

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 Chapter 4 of this Part, 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 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

22 July 2026

---

22 July 2026

PUBLISHED BY AUTHORITY OF THE HOUSE OF LORDS