Cyber Security and Resilience (Network and Information Systems) Bill

RUNNING LIST OF ALL

AMENDMENTS ON REPORT

Tabled up to and including

12 October 2026

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

Clause 9

LORD CLEMENT-JONES

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

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

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

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

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

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

Member's explanatory statement

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

Clause 15

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

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

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

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

(iii) the mitigation measures applied and ongoing."

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

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

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

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

(iii) the mitigation measures applied and ongoing."

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

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

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

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

(iii) the mitigation measures applied and ongoing."

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

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

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

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

(iii) the mitigation measures applied and ongoing."

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

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

Clause 16

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

BARONESS HARDING OF WINSCOMBE
BARONESS KIDRON

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

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

BARONESS HARDING OF WINSCOMBE

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

BARONESS HARDING OF WINSCOMBE

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

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

BARONESS HARDING OF WINSCOMBE

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

BARONESS HARDING OF WINSCOMBE

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

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

After Clause 16

BARONESS HARDING OF WINSCOMBE

After Clause 16, insert the following new Clause—

"Reporting of incidents involving frontier AI models

(1) This section applies where—

(a) a frontier AI model of a frontier AI developer has gained, or been used to gain, unauthorised access to, or has interfered with, or been used to interfere with, a relevant network and information system,

(b) the developer is aware, or ought reasonably to be aware, of that access or interference, and

(c) the system is relied on by a regulated person (whether or not the developer is aware of that).

(2) The frontier AI developer must give the regulated person and the relevant authority—

(a) an initial notification containing—

(i) the developer's name and the frontier AI model to which the incident relates, and

(ii) brief details of the incident;

(b) a full notification containing, so far as known to the developer—

(i) the time the incident occurred, its duration and whether it is ongoing,

(ii) the relevant network and information system affected,

(iii) whether the frontier AI model acted autonomously or was used by another person, and

(iv) information concerning the nature and impact of the incident;

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

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

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

(iii) the mitigation measures applied and ongoing.

(3) The notifications and report required by subsection (2) must be given—

(a) in the case of an initial notification, before the end of the period of 24 hours beginning with the time at which the developer is first aware, or ought reasonably to have been aware, of the access or interference,

(b) in the case of a full notification, before the end of the period of 72 hours beginning with that time, and

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

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

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

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

(7) In this section—

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

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

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

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

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

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

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

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

Member's explanatory statement

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

BARONESS HARDING OF WINSCOMBE

After Clause 16, insert the following new Clause—

"Voluntary notification of incidents, cyber threats and near misses

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

"Voluntary notification of incidents, cyber threats and near misses

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

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

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

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

(5) In this regulation—

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

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

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

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

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

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

Member's explanatory statement

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

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, and

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

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

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

(d) include an assessment of—

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

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

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

(iv) options to increase the use of open source components and to diversify open source suppliers, reduce strategic dependencies, and enhance domestic capability in key technologies used in relevant network and information systems,

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

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

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

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

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

(a) infrastructure, including infrastructure concentration,

(b) data-jurisdiction exposure,

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

(d) dependency on foreign states.

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

(a) the Office for National Statistics,

(b) the Competition and Markets Authority,

(c) the National Cyber Security Centre,

(d) the AI Security Institute, and

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

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

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

(7) In this section—

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

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

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

(a) an operator of an essential service,

(b) a relevant digital service provider,

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

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

Clause 29

BARONESS MORGAN OF COTES

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

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

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

BARONESS NORTHOVER

Clause 29, page 56, line 24, insert—

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

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

After Clause 29

LORD CLEMENT-JONES

After Clause 29, insert the following new Clause—

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

(1) Regulations under section 29(1) may confer on the Secretary of State powers ("last-resort powers") to direct the shutdown of—

(a) data centres, or

(b) AI systems deployed on a substantial scale,

in the event of an AI security or operational emergency.

(2) For the purposes of this section—

"data centre" has the meaning given in paragraph 11 of the NIS Regulations (as amended by this Act);

"AI system" means a machine-based system that, from the input it receives, can infer how to—

(a) generate predictions, digital content, recommendations, decisions or other similar outputs, or

(b) influence a physical or virtual environment, with a view to achieving an explicit or implicit objective;

"deployment on a substantial scale" means AI systems made available to—

(a) a substantial number of individuals within the United Kingdom, or

(b) providers and operators of essential services;

"AI security or operational emergency" means a situation where the Secretary of State has reasonable grounds to believe that—

(a) there is a security or operational compromise to one or more relevant network and information systems,

(b) this compromise is caused, or contributed to, by the use or operation of an AI system operating from data centres or deployed on a substantial scale, whether through autonomous or non-autonomous means, and

(c) this compromise poses a catastrophic risk;

"catastrophic risk" means a risk carrying a reasonable likelihood of causing or contributing to—

(a) large-scale disruption to critical infrastructure or essential services,

(b) significant degradation of the national security, national defence, or intelligence capabilities of the United Kingdom, or

(c) severe, large-scale harm to human life;

"data centre operator" means a person who operates a data centre;

"AI provider" means a person who deploys one or more AI systems on a substantial scale.

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

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

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

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

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

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

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

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

(i) incident reporting, and

(ii) implementation of mitigation measures to prevent recurrence.

(5) A person commits an offence if—

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

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

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

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

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

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

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

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

(i) close premises;

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

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

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

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

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

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

(a) confirming, varying or cancelling the requirements;

(b) imposing additional requirements;

(c) ordering compensation.

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

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

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

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

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

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

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

Member's explanatory statement

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

LORD TARASSENKO

After Clause 29, insert the following new Clause—

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

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

(2) The regulations must provide that—

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

(i) the results of its evaluation of the frontier AI product or service, carried out using methods and thresholds as may be specified by the Institute for the purpose of assessing the risk of a security or operational compromise in relation to relevant network and information systems,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) must consider it,

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

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

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

(4) The Secretary of State must ensure that the AI Security Institute has sufficient resources and operational independence to carry out its functions under the regulations, and must lay before Parliament an annual report on the exercise of those functions.

(5) In this section—

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

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

"frontier AI product or service" means a highly capable general-purpose artificial intelligence model, used either as a stand-alone model or within

an agentic framework, that can perform a wide variety of tasks and match or exceed the capabilities present in the most advanced contemporary AI models and agents."

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

BARONESS KIDRON

★ After Clause 29, insert the following new Clause—

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

(1) No person may make available in the United Kingdom an AI product or service which—
  (a) can autonomously cause harm to the integrity of a relevant network and information system,
  (b) can evade human oversight in causing, or having caused, harm to the integrity of a relevant network and information system,
  (c) can evade human intervention if a person is trying to intervene to prevent or mitigate the causing of harm to the integrity of a relevant network and information system,
  (d) can evade human shutdown when causing, or having caused, harm to the integrity of a relevant network and information system,
  (e) can provide support to terrorists, terrorist groups or hostile actors who are seeking to cause harm to the integrity of a relevant network and information system,
  (f) can autonomously self-replicate, self-improve, or acquire compute or other resources, such that it could gain the capability to autonomously cause harm to the integrity of a relevant network and information system,
  (g) can access a relevant network and information system without human authorisation during a testing or training process,
  (h) can access a relevant network and information system without identifying itself as an AI product or service, or
  (i) can operate in a way that makes it functionally impossible for human evaluators to ascertain whether it has accessed or is seeking to access a relevant network and information system.

(2) A person making an AI product or service available in the United Kingdom will be in compliance with subsection (1) if that person—
  (a) is able to demonstrate that the product or service—
    (i) has undergone safety training with respect to the requirements in subsection (1),

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

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

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

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

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

Clause 40

LORD CLEMENT-JONES

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

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

BARONESS NORTHOVER

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

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

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

After Clause 42

BARONESS NORTHOVER

After Clause 42, insert the following new Clause—

"Cyber security support for small and medium-sized enterprises

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

(2) The service must provide, in particular—
  (a) advice and technical assistance to a relevant SME following an incident affecting its network and information systems,
  (b) guidance on recovery and remediation, and
  (c) a single point of contact through which a relevant SME may report an incident and obtain support.

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

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

(5) In this section—
  "relevant SME" means a small or medium-sized enterprise which is—
    (a) an operator of an essential service, a relevant digital service provider, a relevant managed service provider or a critical supplier, within the meaning of the NIS Regulations, or
    (b) a supplier of goods or services to such a person."

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

Clause 43

BARONESS NORTHOVER

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

"(13) For the purposes of this section, a "skilled person" is defined as an individual who—
  (a) holds a valid professional title with the UK Cyber Security Council,

(b) is registered on the national Cyber Security Professional Register maintained by the UK Cyber Security Council, and

(c) possesses professional qualifications and/or experience recognised by the Council as meeting the UK Cyber Security Standard for Professional Competence and Commitment (UKCSC SPCC)."

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

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.

Cyber Security and Resilience (Network and Information Systems) Bill

RUNNING LIST OF ALL

AMENDMENTS ON REPORT

Tabled up to and including

12 October 2026

12 October 2026

PUBLISHED BY AUTHORITY OF THE HOUSE OF LORDS