Cyber Security and Resilience (Network and Information Systems) Bill

AMENDMENTS

TO BE MOVED

IN GRAND COMMITTEE

[Supplementary to the Marshalled List]

Amendment No.

Clause 12

LORD ARBUTHNOT OF EDROM
LORD CLEMENT-JONES

15A★ Clause 12, page 10, leave out lines 27 and 28 and insert—

"(a) P supplies goods or services, whether directly or through one or more intermediaries, on which an OES for which the authority is the designated competent authority materially depends for the provision of an essential service,"

Member's explanatory statement
This amendment would allow regulators to address material dependencies beyond immediate contractual suppliers, while ensuring that the statutory review tests whether supply-chain risks outside the regulatory perimeter are undermining resilience and does so at a frequency that reflects technological and threat-related change.

LORD ARBUTHNOT OF EDROM
LORD CLEMENT-JONES

15B★ Clause 12, page 11, leave out line 13 and insert—

"(a) P supplies goods or services, whether directly or through one or more intermediaries, on which an RDSP or an RMSP materially depends for the provision of a relevant digital service or managed service,"

Member's explanatory statement
This amendment would allow regulators to address material dependencies beyond immediate contractual suppliers, while ensuring that the statutory review tests whether supply-chain risks

outside the regulatory perimeter are undermining resilience and does so at a frequency that reflects technological and threat-related change.

After Clause 24

BARONESS BERGER

81A★ After Clause 24, insert the following new Clause—

"Education sector to be specified as 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 the provision of education as an essential activity.

(2) Regulations under subsection (1) must, in particular, specify the following as essential activities—

(a) the setting, marking or awarding of qualifications by an awarding organisation recognised by Ofqual or an equivalent regulator in Scotland, Wales or Northern Ireland;

(b) the provision of higher education by a provider registered with the Office for Students or an equivalent UK regulator, including institutions which hold or have access to research, data, or intellectual property whose compromise would be likely to prejudice the national security, economic interests, or research capability of the United Kingdom;

(c) the provision of further education by a provider, including sixth form colleges and providers of vocational training;

(d) the operation of a centralised admissions service for higher education, including the Universities and Colleges Admissions Service (UCAS);

(e) the provision of primary or secondary education by any education institution which—

(i) is essential to the operation of schools in the United Kingdom, and

(ii) processes or holds a significant volume of personal data relating to students or staff.

(3) In specifying an activity under this section, the Secretary of State must have regard to the extent to which network and information systems relied on in connection with that activity are exposed to the risk of a security or operational compromise.

(4) Regulations made under this section must designate appropriate regulatory authorities for the activities specified."

Member's explanatory statement

This amendment requires the Secretary of State to specify the provision of education as an essential activity under Part 3, including any institution that provides primary, secondary, further or higher education or vocational training, and other bodies that are critical to the operation of those education providers, or those that hold student and staff data, or research or intellectual property.

After Clause 35

VISCOUNT CAMROSE
LORD MARKHAM

92A★ After Clause 35, insert the following new Clause—

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

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

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

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

(4) Any report published under this section must include—

(a) an overview of the criteria used to determine strategically important entities, which may include the body's—

(i) turnover,

(ii) number of employees,

(iii) role in the supply of essential goods and services, and

(iv) relevance to the viability of supply chains,

(b) a summary of the reasons why a strategically important entity should be brought within the scope of the NIS Regulations, and

(c) an assessment of further measures needed to address or mitigate risks to the security and resilience of the network and information systems of any strategically important entities that the report concludes should be brought within the scope of the NIS Regulations."

Member's explanatory statement

This new clause would require the Secretary of State to review which strategically important entities not currently within scope of the NIS Regulations should be brought within scope, based on an attack having such a significant impact on the economy or society that they should be considered to be carrying on essential activities.

VISCOUNT CAMROSE
LORD MARKHAM

92B★ After Clause 35, insert the following new Clause—

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

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

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

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

within the meaning of the NIS Regulations.

(4) The guidance required by subsection (1) may require the reporting of—
  (a) whether the business has a cyber security and resilience plan,
  (b) the nature of the cyber security and resilience plan, and
  (c) the use of the cyber security and resilience plan.

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

Clause 40

LORD ARBUTHNOT OF EDROM

95A★ Clause 40, page 63, line 27, leave out "5" and insert "2"

LORD ARBUTHNOT OF EDROM
LORD CLEMENT-JONES

95B★ Clause 40, page 64, line 17, at end insert—

"(f) assess the impact of supply chain and third-party dependencies on the resilience of regulated persons, including where risks originating outside the regulatory perimeter may undermine the effectiveness of the regime."

After Clause 58

VISCOUNT CAMROSE
LORD MARKHAM

174A★ After Clause 58, insert the following new Clause—

"Register of foreign powers for the purposes of Part 4

(1) For the purposes of informing action taken under Part 4 of this Act, the Secretary of State must by regulations made by statutory instrument, and within six months of the day on which this Act is passed, establish and maintain a register of foreign powers that the Secretary of State believes present a risk to the United Kingdom's critical network and information systems.

(2) Foreign powers designated by the Secretary of State under subsection (1) must include states—

(a) which have been confirmed by GCHQ as having—

(i) perpetrated, or attempted to perpetrate, a cyber attack in the UK in the preceding seven years,

(ii) targeted, or intended to target, that attack at the network or information systems of one or more operators of an essential service or critical suppliers, and

(iii) carried out, or intended to carry out, that attack through a state department, agency or affiliate group;

(b) which GCHQ has warned pose a risk to the security or resilience of the network or information systems of one or more operators of an essential service or critical suppliers.

(3) 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.

(4) In this section, "foreign power" means—

(a) the sovereign or other head of a foreign state in their public capacity,

(b) a foreign government, or part of a foreign government,

(c) an agency or authority of a foreign government, or of part of a foreign government,

(d) an authority responsible for administering the affairs of an area within a foreign country or territory, or persons exercising the functions of such an authority, or

(e) a political party which is a governing political party of a foreign government.

(5) A political party is a governing political party of a foreign government if persons holding political or official posts in the foreign government or part of the foreign government—

(a) hold those posts as a result of, or in the course of, their membership of the party, or

(b) in exercising the functions of those posts, are subject to the direction or control of, or significantly influenced by, the party."

Member's explanatory statement
This amendment would require the Government to maintain a register of state actors posing a threat to UK cyber security for the purposes of exercising the Secretary of State's powers under Part 4 of the Act, which enable the giving of directions in the interests of national security.

VISCOUNT CAMROSE
LORD MARKHAM

174B★ After Clause 58, insert the following new Clause—

"Register of foreign powers for the purposes of Part 4: review of nature of risk

(1) For each foreign power added to the register established under section (*Register of foreign powers for the purposes of Part 4*), the Secretary of State must review the extent and nature of the risk posed to the network and information systems of operators of essential services and critical suppliers, including whether the risk arises from—

(a) activities undertaken outside of the United Kingdom, or

(b) foreign owned or controlled infrastructure or locations within the United Kingdom.

(2) Within six months of the establishment of the register under section (*Register of foreign powers for the purposes of Part 4*)(1), the Secretary of State must lay before Parliament a report containing—

(a) the findings and conclusions of the review conducted under subsection (1) above, and

(b) the Government's plan for addressing the risks identified.

(3) If the Secretary of State considers that laying a report, or any portion of a report, under subsection (2) would be contrary to the interests of national security, the Secretary of State must make a statement to Parliament confirming that—

(a) a review has been conducted under subsection (1), and

(b) that the report, or a portion of the report, cannot be laid before Parliament for reasons of national security."

Member's explanatory statement
This new clause would require the Government to conduct a review and report to Parliament on the risk to relevant network and information systems posed by foreign powers appearing on the register established by the new clause "Register of foreign powers for the purposes of Part 4", considering whether such risks arise from extra-territorial activities and infrastructure or premises owned or controlled by foreign powers.

LORD ARBUTHNOT OF EDROM

174C★ After Clause 58, insert the following new Clause—

"Guidance: skills and competency requirements

The Secretary of State must issue guidance setting out the skills and competencies relevant to compliance with duties under this Act relating to the security and resilience of network and information systems, including the role of recognised professional standards and independently assessed competence."

Member's explanatory statement
This amendment would require the Government to publish guidance concerning the capability and skills required for effective implementation of the provisions of this Act.

LORD ARBUTHNOT OF EDROM

174D★ After Clause 58, insert the following new Clause—

"Strategy for developing cyber-security and resilience capability across regulated sectors under this Act

(1) Within 12 months of the day on which this Act is passed, the Secretary of State must publish a strategy for developing cyber-security and resilience capability across the sectors regulated under this Act.

(2) The strategy for regulated sectors published under subsection (1) must include workforce development, training and professional standards.

(3) The Secretary of State must publish an updated strategy in each calendar year."

VISCOUNT CAMROSE
LORD MARKHAM

174E★ After Clause 58, insert the following new Clause—

"Increasing resilience by reducing data retention

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

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

Cyber Security and Resilience (Network and Information Systems) Bill

AMENDMENTS

TO BE MOVED

IN GRAND COMMITTEE

[Supplementary to the Marshalled List]

28 August 2026