



Department for
Digital, Culture,
Media & Sport

The Baroness Lloyd of Effra
Parliamentary Under-Secretary of State for Space, Cyber and
Regulatory Reform
Department for Digital, Culture, Media and Sport
22-26 Whitehall
London, SW1A 2EG

www.gov.uk/dsit

8 September 2026

Dear Colleagues,

Thank you for your engagement with the Cyber Security and Resilience (Network and Information Systems) Bill during the second of its Committee Stage sessions in the House of Lords.

I agreed to write on questions that were raised by Noble Lords, and responses are outlined below:

1. Does the UK allow extradition to Hong Kong on an ad hoc basis?

Extradition cooperation with Hong Kong remains suspended. Last year's changes to the Extradition Act 2003 strengthened that position by removing Hong Kong's designation under the Act and formally implementing in domestic law the UK's suspension of the 1997 UK-Hong Kong Extradition Treaty. While UK law does not provide for an absolute statutory prohibition on the consideration of ad hoc extradition requests from any particular jurisdiction, any such request would be subject to the stringent safeguards set out in the Extradition Act 2003. UK courts can refuse extradition where it would be incompatible with a person's human rights or where a request is politically motivated. The Government will not permit extradition to be used to suppress democracy, free speech or legitimate political activity and remains committed to protecting the rights and safety of Hong Kongers in the UK.

2. What powers under this Bill will you use to create board responsibility requirements? How will board responsibility requirements be mandated?

Clause 29 enables the Secretary of State to make regulations to strengthen the cyber security and resilience of essential and digital services. We intend to use this power to introduce a set of mandatory security and resilience requirements (SRRs) in secondary legislation.

SRRs will be consistent with the NCSC's Cyber Assessment Framework, and will be outcomes-based, rather than prescriptive controls. We propose to include a specific requirement on regulated entities to ensure that there is appropriate governance, senior responsibility, accountability, and organisational capability to support the protective and preventative measures they must take. We expect that this will include specific duties placed on the board or equivalent senior management, to have nominated accountability for security and resilience, maintain and implement a cyber security policy, and ensure appropriate staff training and effective risk escalation arrangements.

Further details on these proposals will be consulted on later this year, and relevant secondary legislation will be subject to the affirmative procedure.

3. Are customer relationship management services within the scope of this Bill?

A customer relationship management (CRM) provider could fall within scope as a Relevant Managed Service Provider (RMSP) if it meets all of the characteristics of the definition. This would include the organisation having a contract for the ongoing management of a customer's IT systems and having access to – or connection with – those systems as part of a managed service.

However, a CRM could also meet the definition of a cloud computing service and be in scope as a Relevant Digital Service Provider (RDSP). The cloud computing service definition in the NIS Regulations 2018 is designed to capture cloud-based Software-as-a-Service (or SaaS). Therefore, if a CRM system is delivered as a cloud-based software service, or if it provides a cloud hosting service, it may be captured under the regulations as an RDSP. Whether an organisation falls into scope as an RDSP also depends on whether relevant exclusions apply, such as the one for small and micro enterprises.

Finally, if a CRM does not meet either of these definitions but is identified as providing a critical good or service to a regulated entity, it could be designated by the regulator as a critical supplier, subject to meeting the designation criteria.

4. What action is being taken to ensure the cyber security of examining bodies?

Ofqual is the independent regulator of qualifications, examinations and assessments in England. Awarding organisations, including the exam boards offering GCSEs and A levels, are responsible for the secure development, delivery and awarding of qualifications and examinations. Ofqual regulates those organisations and requires them to have appropriate arrangements in place to identify, manage and mitigate risks to the integrity and security of the exams system.

Ofqual requires awarding organisations to establish and maintain effective governance, risk management and contingency arrangements, including arrangements for managing incidents and ensuring business continuity. Awarding organisations must also take appropriate steps to assess and manage risks arising from third-party suppliers and wider supply chains that could affect the secure delivery of qualifications.

The Department for Education works closely with Ofqual and awarding organisations on matters affecting the resilience of the exams system. Ofqual, along with the National Cyber Security Centre, continues to engage with awarding organisations on cyber resilience and preparedness, including convening annual cross-sector scenario planning exercises and working with stakeholders to strengthen preparedness for significant incidents. Awarding organisations are responsible for implementing and maintaining appropriate security controls and response arrangements. All four exam boards offering GCSEs and A Levels

have ISO27001, which is the internationally recognised standard for cyber security management.

In recent years, awarding organisations have enhanced their cyber-security arrangements, including improved monitoring, strengthened controls for third-party suppliers, more secure authentication measures, regular penetration testing and cyber incident exercises to test incident response arrangements.

Protecting students and maintaining the integrity of qualifications is a priority. While these measures strengthen resilience, no system can completely eliminate the risk of a successful cyber attack. For this reason, recovery and contingency planning are also critical. The exams system has arrangements in place both to reduce the likelihood of incidents occurring and to respond appropriately should they occur.

5. Are DCMS officials coordinating with the cyber security group within DHSC, especially related to threats from AI agents? Have the recent reports from AISI been communicated to the cyber security group in DHSC and their implications discussed with them?

DSIT wrote to DHSC on 16 April 26 in relation to the latest developments around AI cyber threats. This letter included reference to the recent work of the AISI.

The Joint Cyber Unit in DHSC/NHSE work closely with the National Cyber Security Centre (NCSC) to assess the likely impacts from the emerging cyber threats, including agentic AI. This work includes working with the Arms Length Bodies of DHSC on the matter. There have been recent forums on the subject with input from NCSC where NHSE and others shared emerging best practice on responding to this new threat.

NHS England is undertaking a programme of work to assess and prepare for the cyber security risks associated with advanced and agentic AI systems. This includes participation in a cross-government initiative evaluating how AI can be applied to vulnerability discovery, security testing and cyber defence. Insights and learning from this work are shared with DHSC and its Arm's Length Bodies.

DHSC/NHSE have produced guidance for frontline NHS organisations to help them deploy AI in a secure manner, reducing the risk of introducing additional cyber risks. This guidance included input from DSIT/DCMS and NCSC. DHSC/NHSE AI and Cyber teams share internally AISI reports and findings regularly, and they are reflected in ongoing policy development and operational responses for the health and care sector.

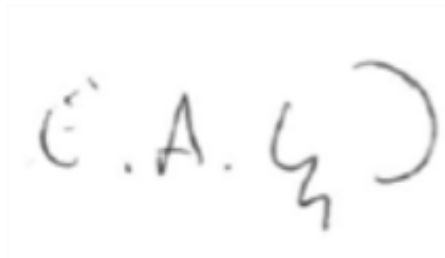
Officials from DHSC/NHSE meet regularly with DCMS colleagues through a number of formal and informal boards and working groups that discuss cyber security matters.

6. Has DCMS assessed the risk of technological dependence on foreign companies managing personal data in the NHS to relevant network and information systems?

Risks associated with technology suppliers are considered through established security and resilience processes. Procurement decisions are taken on the basis of value for money, security and the effective delivery of public services. Decisions affecting critical infrastructure are informed by evidence relating to security, reliability and long-term resilience.

I hope these answers provide the clarification that you are seeking.

Yours sincerely,

A handwritten signature in dark ink, appearing to read 'E.A. Lloyd', enclosed within a faint rectangular border.

Baroness Lloyd of Effra
Parliamentary Under-Secretary of State for Space, Cyber and Regulatory Reform
Department for Digital, Culture, Media and Sport