Law Society of Scotland

Second Reading Briefing

(House of Lords)

Cyber Security and Resilience (Network and Information Systems) Bill

July 2026

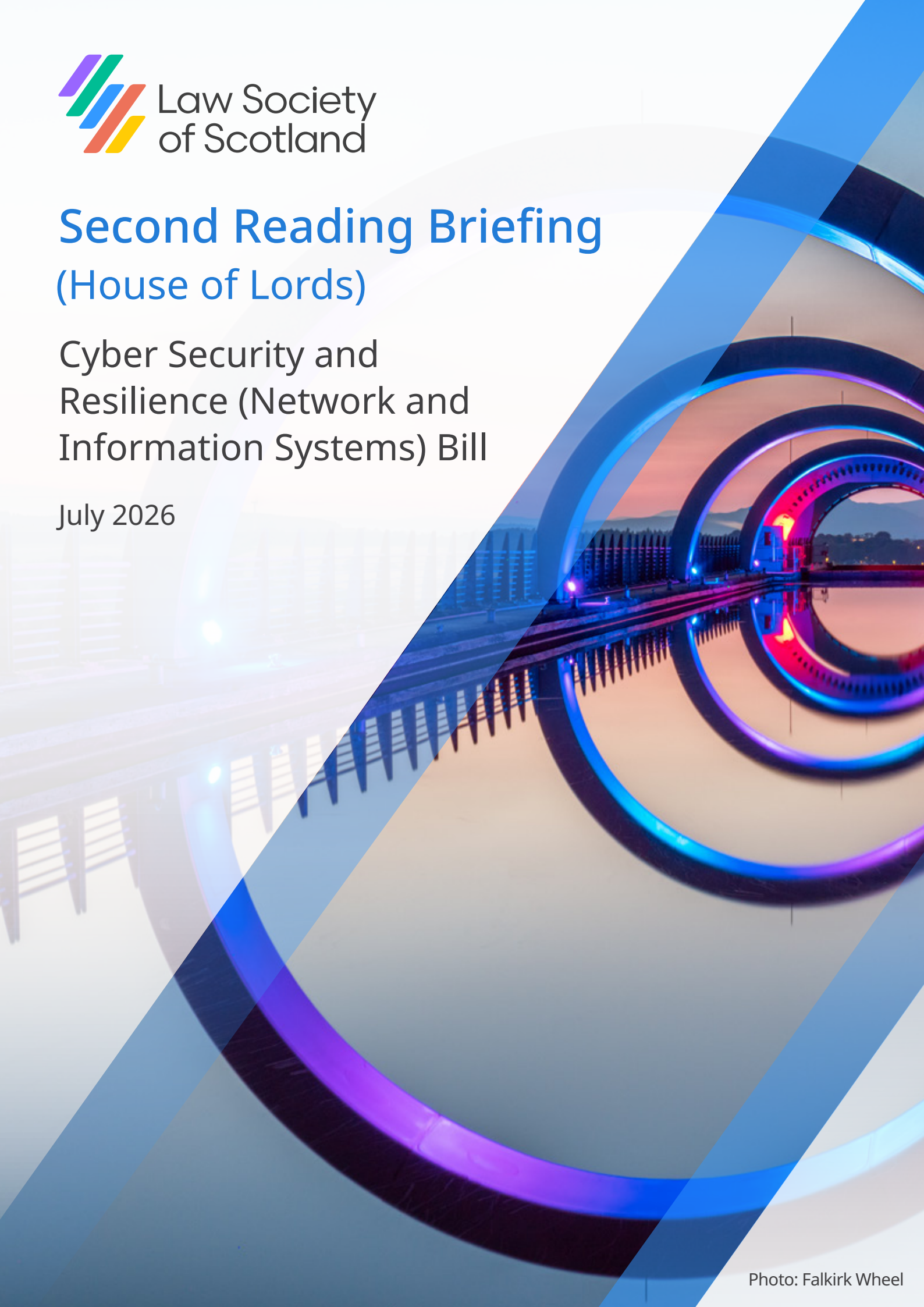

Photo: Falkirk Wheel

Law Society of Scotland

Cyber Security and Resilience (Network and Information Systems) Bill

Second Reading (House of Lords)

July 2026

Introduction

The Law Society of Scotland is the professional body for over 13,000 Scottish solicitors.

We are a regulator that sets and enforces standards for the solicitor profession which helps people in need and supports business in Scotland, the UK and overseas. We support solicitors and drive change to ensure Scotland has a strong, successful and diverse legal profession. We represent our members and wider society when speaking out on human rights and the rule of law. We also seek to influence changes to legislation and the operation of our justice system as part of our work towards a fairer and more just society.

The Cyber Security and Resilience (Network and Information Systems) Bill (**Bill**)[1] was introduced to the House of Commons on 12 November 2025. The Bill seeks to reform the UK's only cross-sector cyber security regulations (the "**NIS Regulations"**[2]) and extend cyber security requirements to a wider range of sectors and services critical to the UK economy. It also introduces stricter incident reporting and oversight measures to improve the resilience of key infrastructure.

Our Privacy Law sub-committee welcomes the opportunity to provide comments ahead of the Second Reading on 14 July 2026. Our briefing contains the following key points:

- We welcome the Bill's attempts to strengthen cyber-security in the UK but believe that the legal profession and wider business community also have a part to play in tackling this issue.
- We support a need to undertake wider stakeholder consultation in terms of the secondary legislation that will implement this Bill.
- We believe that effective legal safeguards need to be in place should powers to disclose sensitive personal information on grounds of national security be agreed in this Bill.

We also have the following substantive comments to put forward for consideration.

General Remarks

We note that the Bill makes updates to the NIS Regulations and will deliver powers to ensure that the Government can respond to new and emerging cyber security threats. To achieve this, the proposed reforms to the NIS Regulations place cyber security requirements on operators of essential services including drinking water, health, energy, transport and digital infrastructure as well as relevant digital

[1] Cyber Security and Resilience (Network and Information Systems) Bill
[2] The Network and Information Systems Regulations 2018

service providers. We consider that these sectors are essential to the day-to-day functioning of a healthy society in Scotland.

We also recognise the importance of effective cyber security mechanisms to enable growth and stability in the economy. The need for this should not be understated given recent figures demonstrate that cyber threats continue to be a very real threat to the country and wider economy[3]. These concerns are heightened by views shared by the National Cyber Security Centre who point to *"state actors continuing to present a significant threat to UK and global cyber security, aided by an ever evolving cyber intrusion sector."*[4]

In view of these points, we welcome the Bill's attempts to combat the issue of cyber security. However, we do also recognise that both the legal profession and wider business community have a part to play in tackling this issue. We believe that organisations need to be proactive in ensuring that appropriate controls and safeguards are in place to deal with cyber-security breaches that directly impact them.

We also note that the Bill leaves a significant amount of detail to secondary legislation and associated guidance. We believe that this may pose difficulties for wider industry to plan and provide for the costs of implementing this Bill. However, we also accept that the Bill represents an attempt to deal with cyber threats that are both fast-moving and changing as technology develops by the day. Therefore, we believe that primary legislation may lack sufficient flexibility to quickly deal with new or novel cyber security threats.

We therefore see it as crucial that wider consultation takes place on any associated secondary legislation that will implement this Bill, along with sufficient guidance being developed that will sit alongside these provisions. We believe this will assist those organisations affected by the Bill to better understand the wider cyber security obligations they will now be subject to.

Part 1 – Introduction

We have no comments to make on Clauses 1 and 2, which provides a meaning of the NIS Regulations and overview of the Bill.

Part 2 – NIS Regulations

Part 2 is the core operative part of the Bill. It recasts the NIS Regulations by redefining who is regulated and how cyber-risk management and incident reporting is to change. It also provides new powers in terms of regulatory oversight and enforcement, along with introducing new information sharing powers.

[3] Cyber Security Breaches Survey 2022
[4] Chapter 01: Countering the cyber threat | National Cyber Security Centre

Chapter 1 (Clauses 3 to 12 – Persons Regulated under the NIS Regulations)

We note that the Bill will update the NIS Regulations by bringing new entities and services into scope. This includes data centre infrastructure, large load controllers and managed service providers. Alongside this, the Bill will equip regulators with increased powers to designate "critical suppliers", update incident reporting regime requirements, make changes relating to the recovery of costs and provide better information gathering and enforcement powers.

Data Centres

Clause 4 introduces data infrastructure as a sector within the scope of the NIS Regulations. It also designates the Secretary of State and Ofcom as joint regulators of this space.

We accept the need to bring data centres into scope given how critical these are to the economy, national security and thus wider society. For example, data centres undertake a host of important functions including retaining NHS patient records and diagnostics, various financial services including payments and trading, as well as providing cloud services and national connectivity. As a result (and given that data centres were formally designated as Critical National Infrastructure in 2024[5]), the absence of mandatory statutory oversight of data centres in the NIS framework would arguably be a regulatory gap.

However, we believe it is important that clear boundaries are drawn in order to minimise the risk of duplicative or overlapping regulation. Data centre operators are already subject to GDPR and data protection obligations in relation to any personal data that they process.

We also believe that further guidance should be provided as to how organisations should prioritise incident and notification requirements or obligations when subject to multiple requests from enforcement agencies, including both the Information Commissioner's Office and Ofcom.

Managed Service Providers

We note that Clause 9 amends Regulation 1 of the NIS Regulations to insert a definition of a *"*relevant managed service provider"[6] (**RMSP**) and "managed services."[7]

We believe that the definition of a RMSP contained in the Bill is too broad and will likely lead to providers with only peripheral or low risk involvement being captured. For example, the Bill does not define what a core managed IT service actually is: for example, is this the provision of an IT outsourcing SaaS, cloud or IT

[5] See Policy Paper - Data centres – Department for Science, Innovation and Technology
[6] See Clause 9(4) of the Cyber Security and Resilience (Network and Information Systems Bill inserting a new paragraph (ea) in Regulation 1, paragraph (3), sub-section (e)
[7] Ibid - See sub-section (5)

infrastructure service? Certain organisations may therefore struggle to tell from the statutory language alone whether they are captured by the Bill, particularly if they provide IT services that are ancillary to a wider offering, or if the services they provide are limited in scope.

In view of this, we believe that the Bill could include clear statutory thresholds through a closed list of criteria for RMSP inclusion such as the scale of a business' operations, the number of regulated customers they have or the sensitivity or criticality of the systems that they manage. Without clear statutory scoping, we believe that legal certainty may arise in the identification of RMSP's that fall under the provisions of this Bill.

The Designation of Critical Suppliers

We note that Clause 12 amends the NIS Regulations to insert a new Part 4B, which provides a framework for the designation, regulation and oversight of "critical suppliers". This provision also confers extended powers on sector regulators in the designation process.

We believe that this provision also lacks a detailed set of criteria allowing for the identification of a critical supplier. For example, it is not clear from the Bill whether a supplier is in scope at an organisational level or in context of the service they provide. We believe that this may lead to legal uncertainty for organisations that provide multiple services which span different categories. We consider that this could risk arbitrary designation which, in turn, may undermine wider confidence in the regulation of this space. Additionally, we believe that inconsistent application of these provisions could also risk stifling innovation within this supply base due to a lack of predictability and uncertainty in terms of the scope of the provisions. In situations where critical suppliers face an inconsistent application of the provisions, multiple compliance processes, legal reviews and reporting arrangements may direct resources away from research, development and cyber-resilience improvements to their organisations.

Chapter 2 (Clauses 13 to 16 – Provision of Information and Reporting of Incidents)

Incident Reporting

Clause 15 amends Regulation 1(2) of the NIS Regulations to capture cyber security incidents that are "capable of having" a significant impact on the security of network and information systems.

We believe that the term "capable of having"' is ambiguous and open to interpretation. For example, any phishing email is technically "capable of" having a significant impact on an organisation if it lacks adequate detection or response.

In view of this, we believe that the Bill risks capturing a wide range of incidents given that service providers are being asked to provide a subjective assessment of a hypothetical future impact rather than a current and direct observable harm.

We believe that this could lead to an over-reporting of low-level incidents, in turn overburdening regulators and thus distracting attention from genuinely significant threats. This issue is likely to be exacerbated by strengthened enforcement powers of sector regulators under the Bill, and thus likely encourage over reporting as a cautious approach.

In view of this, we would make two suggestions:

(1) that further clarity is provided through an explanatory note as to what is expected under this provision, and that this addresses instances which are deemed to be "capable of having a significant impact"; and / or
(2) That the phrase used is one more familiar with either being "unlikely to result in a risk" or "is likely to result in a high risk" which mirrors the language used in Article's 33 and 34 of the UK GDPR[8].

We believe either of those changes will address the challenge of ensuring that incident reporting will be properly understood across all sectors.

We also note that Clause 15 introduces a mandatory "initial notification" of becoming aware of a qualifying incident, followed by a fuller report within 72 hours. We have reservations as to whether 24 hours is a sufficient time-period to allow organisations to seek competent legal advice in determining whether the statutory threshold for notification has been met.

We do, however, acknowledge the need for the timely notification of a cyber security attack.

Information Sharing

Clause 18(3) amends information sharing provisions under Regulation 6 of the NIS Regulations. This creates new information sharing gateways allowing NIS enforcement authorities to share information obtained under the regime with other UK public authorities, and certain overseas authorities.

We do see certain strengths in these provisions which include the apparent need to address the inability of regulators to share relevant intelligence or information that is directly relevant to national security and serious crime.

However, we believe that these provisions also provide an avenue for wider confidential data to be shared including sensitive customer information of a business which could be open to misuse.

In view of this, we stress the need for further information to be provided which will outline an expectation on NIS enforcement agencies to carry out data protection impact assessments (or some other form of safeguard) to address both the

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation)

necessity and proportionality of sharing data before it is disclosed. NIS enforcement agencies should also consider whether the sharing of information can be just as effective if anonymised.

Chapter 3 (Clauses 17 to 23 – Other Amendments)

We have no comments to make on these provisions.

Part 3 – Security and Resilience of Systems: Functions of the Secretary of State

Part 3 provides the governance section of the Bill and sets out how the regime will adapt over time. In doing so, this Part provides the Secretary of State with powers to set strategic priorities, initiate the use of codes of practice to guide compliance with the Bill and allow the framework to be updated via secondary legislation. It is hoped that this Part will assist regulators and regulated entities how to interpret and apply their duties.

Chapter 1 (Clause 24 – Introductory)

We have no comments on the key definitions contained at Clause 24.

Chapter 2 (Clauses 25 to 28 - Statement of Strategic Priorities etc)

We have no comments to make on these provisions.

Chapter 3 (Clauses 29 to 35 - Regulations About Security and Resilience of Systems)

We have no comments to make on these provisions.

Chapter 4 (Clauses 36 - 39 Code of Practice)

Clause 36 sets out that the Secretary of State may issue a code of practice for regulated persons outlining the recommended steps to enable compliance with the duties imposed under the Bill.

We support the aim of translating statutory duties into operationally meaningful expectations. We believe that this will reduce uncertainty for regulated entities about what will constitute effective compliance in practice.

However, we believe that detailed consultation will be required in the development of any code of practice and that this should be undertaken prior to issuing a code.

With this in mind, we welcome the requirement under sub-section (3) for the Secretary of State to undertake statutory consultation with relevant stakeholders. At the same time, we have concerns as to the way in which this requirement has been framed in that it imposes a requirement to “consult with such persons as the Secretary of State considers appropriate”. We believe that this drafting is vague and risks inconsistent or insufficient engagement with those operating in affected sectors.

In view of this, we welcome the further safeguards that are provided at Clause 37(1) and (2) which ensure that a draft code must be laid before Parliament. It also provides for a 40-day objection period which will allow either House to block the code. We support this provision and believe any debate over the code will provide for transparency as to how a Minister of the executive has developed the code.

Chapter 5 (Clause 40 – Report on Network and Information Systems Legislation)

We have no comments to make.

Chapter 6 (Clauses 41 to 42 - Regulations under Part 3)

We have no comments to make.

Part 4 – Directions for National Security Purposes

Part 4 of the Bill creates new powers for the Secretary of State to intervene in a cyber security threat that poses a serious threat to national security where this cannot be addressed through ordinary regulator-led supervision alone.

As part of this, Clause 56 sets our further provision for when the Secretary of State or sector regulators can disclose information for national security purposes. We have concerns that this provision grants the Secretary of State direct and binding powers over both regulated entities and independent regulators. This represents a concentration of power with the Secretary of State in an area that had been traditionally regulator-led, and at arms length from the executive.

As a result, we believe that it is important that a robust set of checks are put in place that will ensure that these powers are, and have been, exercised in accordance with the law. We do, however, recognise the difficulties and challenges that may arise in the disclosure of information when operating in instances of national security.

Part 5 – General

Part 5 of the Bill does not introduce new cyber security duties or enforcement powers, but instead addresses how the substantive parts of the Bill operate legally, territorially and procedurally. It also looks at how the Bill will integrate with the existing NIS framework.

We have no comments to make on these provisions.

For further information, please contact:

Richard Visocchi
Policy Executive
Law Society of Scotland
DD: 0131 476 8113
richardvisocchi@lawscot.org.uk