Written evidence submitted by ISC2 (CSRB10)

Cyber Security and Resilience (Network and Information Systems) Bill – Public Bill Committee Submission

ISC2

ISC2 is the world's leading member association for cybersecurity professionals. Our more than 265,000 certified members, and associates, lead the profession with the same shared vision: a safe and secure cyber world. ISC2's membership includes 10,000 members in the UK. ISC2 is a Founding Member of the UK Cyber Security Council, has worked with the Department for Science, Innovation and Technology on various Codes of Practice, and is a supporter of the National Cyber Security Centre's CyberFirst programme.

ISC2 supports the intention of the Cyber Security and Resilience (Network and Information Systems) Bill. This Submission provides feedback on the Bill from ISC2, informed by views from ISC2's UK members.

The first section of this submission concerns specific amendments to strengthen, clarify and add to the Bill, while the second section comments more broadly on the Bill.

Amendments

Strengthen the Bill

Clause 43 on national security directions references a 'skilled person' an organisation must appoint to liaise with the Secretary of State to comply with a national security direction. The Bill must define what qualifies as a skilled person under this provision, allowing organisations and professionals to prepare.

ISC2 would recommend that the Bill be strengthened by adding the definition of a skilled person. The definition should be that a skilled person is an individual who has demonstrated, through competence-based assessment and certification in accordance with ISO/IEC 17024, that they possess the required knowledge, skills, and abilities to perform specific tasks or functions effectively, reliably, and in compliance with defined professional or industry standards.

Clause 40 of the Bill requires that the Secretary of State lay a report before parliament on the operation of the legislation. This review cycle is too slow for such a dynamic policy area, particularly given the extensive use of secondary legislation. Without regular impact assessments, government will lack the feedback needed to judge effectiveness.

ISC2 recommends that the Bill be strengthened by reducing duration of this report to every two years.

Clarify the Bill

Clause 15 of the Bill amends the scope of incidents that must be reported. An incident means any event having or capable of having adverse effect on the security of network and information systems. While the Bill does list factors that should be regarded in determining the significance of an incident, such as number of people affected, geographical spread and economic cost, it provides no benchmarks to judge each factor.

The Bill should clarify incident thresholds, either through the promise of further guidance, or in the primary legislation. The absence of benchmarks risks inconsistent interpretation by regulated entities.

Addition to the Bill

The effectiveness of the implementation of this Bill will depend on the availability of adequate cybersecurity skills for regulated organisations. In already understaffed and pressurised cybersecurity teams, there is a risk that an increased compliance burden will divert resources from critical cyber operations that could prevent future incidents.

ISC2 recommends an addition to the Bill that the Secretary of State must issue guidance on the cybersecurity skills and competencies relevant for compliance with duties under this Act and publish an action plan for how the government will support organisations prepare their workforce.

As a principle, ISC2 would like to see the government engage with industry and cybersecurity professionals through every stage of this Bill, including the introduction of Secondary Legislation attached to it.

On the Bill

The Cyber Security and Resilience (Network and Information Systems) Bill continues the UK's cybersecurity regulatory path of mandating cybersecurity duties only on critical national infrastructure, defining this as operators of essential services, digital service providers, managed service providers and critical suppliers of essential services. The Bill serves as an update on the previous Network and Information Systems (NIS).

This document provides five themes, outlining ISC2's positions on the Bill in its current state:

Preparedness

Government should ensure that both businesses and regulators are adequately prepared to meet the obligations created by the Bill. As a first step it should determine which cybersecurity skills and roles will be necessary to ensure effective compliance with the Bill, and ensure resource and process are in place to develop those skills across relevant organisations.

We know that skills shortages exist and impede compliance with regulations. ISC2's 2025 Cybersecurity Workforce Study reports that almost **88% of respondents experienced at least one cybersecurity breach as a result of skills shortages, with 95% reporting at least one skills need in their organisation** while showing that skills shortages are the number one challenge in the UK for complying with regulations (47%).

Organisations will also need clarity on what duties they will have to comply with. The Bill in its draft form, does not expand the duties on organisations further than the previous regulations. It does however allow for new codes of practice and provides significant scope for new guidance from the regulators. Despite no new duties being outlined in the Bill, much of the commentary suggests there will be an expanded role for supply chain resilience. Government should provide clarity on what will be expected of organisations to allow time to prepare.

It is also necessary for **regulators to have the capacity** to carry out their expanded role. However, regulators face a structural problem: they require additional resources to fulfil the expanded duties set out in the Bill, yet those resources are only unlocked by the Bill itself. Government should clarify how this will be resolved and set out a clear plan for resourcing regulators ahead of implementation.

While the Bill itself contains no extra duties on regulated bodies, it is expected that new guidelines will include stronger supply chain resilience for critical national infrastructure. This will include SMEs in the supply chain, which are time and resource poor, ad often unable to access or develop cybersecurity expertise. Therefore in preparation for this Bill, and to ensure the cyber resilience of the supply chains of critical infrastructure, the government should commit to a ringfenced fund for SMEs, allowing them to access or develop cybersecurity expertise.

- ISC2's 2025 Cybersecurity Workforce Study reports that almost **88% of respondents experienced at least one cybersecurity breach as a result of skills shortages, with 95% reporting at least one skills need in their organisation** while showing that skills shortages are the number one challenge in the UK for complying with regulations (47%).
- Government must clarify how regulators will create capacity to carry out duties contained within the Bill, given the current measures to create capacity are a result of carrying out those same duties.
- Government should provide clarity on what duties will be expected of organisations to allow time to prepare, including whether they need to increase supply chain resilience.
- In 2021 Ofcom received an increased budget from the government due to its expanded rules under the Telecommunications Security Act 2021.[1] This should act as a model for the government to provide upfront funding to build regulator capacity.
- The government should commit to a ringfenced fund for SMEs to access or develop cybersecurity expertise, helping secure the resilience of supply chains.

[1] From a written Parliamentary Question: "The Ofcom security budget for this financial year has been increased by £4.6 million. This funding will allow Ofcom to more than double the number of staff working on telecoms security by the end of this financial year. This includes hiring a multi-skilled team including technical, enforcement and legal experts."

Incident reporting

The Bill risks a further fragmented reporting framework. Though the reporting timelines are standardised, organisations must report incidents to their sectoral regulator rather than through a central national platform. For those with multiple regulators, this may result in duplicated reporting obligations. When combined with UK GDPR requirements or sector specific regulators or guidelines such as the Financial Conduct Authority guidelines or the Telecommunications (Security) Act 2021, organisations may face multiple separate reporting routes and thresholds.

Further complicating matters, many organisations under scope of the Bill will operate internationally, so will have to comply with reporting obligations in other jurisdictions, such as under NIS2 in the EU. This means one incident could trigger several reporting schedules and formats, removing resources from effectively responding to the incident itself.

We recommend a clear call to action: **government should streamline incident reporting and move towards a unified reporting platform**.

Government should also provide clarity on the threshold for reporting. The draft Bill refers to "significant" incidents and lists criteria such as service disruption, number of users affected, duration, geographic impact, and effects on data confidentiality, integrity, authenticity or availability. It does not specify whether meeting any one of these criteria is sufficient, nor who or what determines significance. Clear, operational definitions are essential to support compliance.

- Government should move towards a unified incident reporting system, covering incidents that need to be reported to multiple regulators or under multiple legislative requirements.
- Either through an amendment or further guidance, government should provide clarity on the criteria for when an incident is 'significant'.

National Cyber Action Plan

The Cyber Security and Resilience Bill and the forthcoming National Cyber Action Plan must be aligned and mutually reinforcing. This is essential for delivering a strategic approach to national resilience. The National Cyber Action Plan does provide an opportunity to be an anchor for the legislative framework, including for the guidance and Secondary Legislation that must follow this Bill for effective implementation.

Government should use the National Cyber Action Plan to set out a robust policy and legislative framework — including measures to professionalise the cybersecurity workforce — and avoid missing a rare opportunity to strengthen the UK's long-term resilience.

Under the Bill's sections on national security directions, a regulated body is required to appoint 'a person with expertise in relation to the security of network and information systems (a "skilled person")', for the purposes of assisting the regulated body with the direction. Defining a "skilled person" under the Bill could be a first step to professionalising the sector. This should be grounded

in internationally recognised standards, such as ISO/IEC 27021, to support international interoperability and competency assurance.

- The government should use the upcoming National Cyber Action Plan to set out a robust policy and legislative framework.
- This should include professionalising the sector, starting with defining what a 'skilled' person means in the Cyber Security and Resilience Bill, and grounding this in internationally recognised standards, such as ISO/IEC 27024.

Impact assessment

Reviews should be an active part of the legislative cycle, particularly in a fast-evolving domain such as cybersecurity. The Bill currently requires the Secretary of State to report on the Bill's operation at least once every five years. This interval is too long to track effectiveness or respond to shifting threat landscapes.

A shorter, more agile review cycle — especially given the Bill's reliance on secondary legislation — is essential. Without regular impact assessments, government will struggle to evaluate the Bill's performance or adapt policy in a timely way.

- The Bill as drafted compels the Secretary of State to report to parliament every five years "on the operation of the legislation"; this interval is far too long to track effectiveness.
- Reviews of policy effectiveness should be an active part of the legislative cycle, starting with shorter review periods for this Bill.

UK PLC

While the Bill covers operators of essential services, digital service providers, managed service providers and critical suppliers, a substantial proportion of the UK economy falls outside its scope. As a result, the Bill would not have mitigated recent attacks on high-profile UK businesses such as Marks & Spencer, Co-op or Jaguar Land Rover, as the manufacturing and retail sectors are not covered by the sectoral scope of the Bill.

Another critical sector not covered by the Bill is public administration. This means there are no measures to improve the cybersecurity and resilience of public administration organisations, such as local authorities, government departments and agencies. One cannot expect a fully cyber resilient nation without securing all parts of it. We expect the Government Cyber Action Plan to address this issue.

The National Cyber Action Plan must therefore set out a broader suite of interventions to strengthen the resilience of UK PLC. This should include wider adoption of existing codes of practice, the promotion and design of cybersecurity standards, and the use of procurement and fiscal levers to support business investment in cybersecurity — echoing recommendations from the Business and Trade Committee's report on economic security. As the government's own impact assessment notes, "the cost of doing nothing is too great".

SMEs in particular do not have the skills available or depth of personnel to adopt a strong cybersecurity posture and comply with regulations. Any effort at national cyber resilience must include a ringfenced fund to help SMEs build or access the required cybersecurity expertise.

- This Bill does not cover the majority of UK business, or public administration.
- To improve national resilience, the government should use non-legislative measures such as codes of practice, strong cybersecurity standards, procurement and tax incentives to increase market adoption of cybersecurity practices. The Business and Trade Committee recommended tax incentives for businesses to invest in cybersecurity in its economic security inquiry.[2]

January 2026

[2] https://committees.parliament.uk/publications/50340/documents/272083/default/