Written evidence submitted by UK Cyber Security Council (UK CSC) to the Cyber Security and Resilience Public Bill Committee (CSRB06)

Embedding UK Cyber Security Council Professional Titles into the Cyber Security and Resilience Bill

Cover Note

Purpose: To propose targeted amendments to the Cyber Security and Resilience (Network and Information Systems) Bill [Bill 329, as introduced] that align workforce competence with the professional titles awarded by the UK Cyber Security Council (UK CSC), while preserving the Bill's risk-based and proportionate approach.

Executive summary: The Bill strengthens UK cyber resilience by expanding NIS scope (including RDSPs, MSPs, data centres), enhancing incident reporting, guidance, and regulatory powers. Our amendments introduce consistent "have regard to" language wherever the Bill relies on organisational competence to deliver outcomes—incident response, risk management, designation and oversight—so regulators and operators can rely on a recognised professional architecture for cyber roles.

Policy and evidence alignment: This approach reflects the Government's policy statement and the National Cyber Security Centre's emphasis on closing the capability gap across critical sectors. It also aligns with practice in existing frameworks (e.g., CAF) without mandating any single certification pathway.

Scope of insertions (ordered by clause):

- Clause 8 – Duties of relevant digital service providers (RDSPs)
- Clause 10 – Duties of managed service providers to manage risks
- Clause 11 – Public authority oversight (scope test)
- Clause 12 – Critical suppliers
- Clause 15 – Reporting of incidents by regulated persons
- Clause 16 – Notification of incidents to customers
- Clause 19 – Guidance under the NIS Regulations
- Clause 29 – Regulations relating to security and resilience of systems (enabling power)
- Clause 30 – Imposition of requirements on regulated persons
- Clause 31 – Functions of regulatory authorities (assessment lens)
- Clause 36 – Code of practice
- Clause 47 – Inspections (national security directions)

Impact: Provides a consistent, auditable benchmark for cyber workforce competence across regulated activities; supports proportionate enforcement; reduces ambiguity for mixed public/commercial providers; strengthens incident reporting and customer notifications; and enables future tailoring through secondary legislation and codes of practice.

Key references:

• Cyber Security and Resilience (Network and Information Systems) Bill [Bill 329, as introduced] – https://publications.parliament.uk/pa/bills/cbill/59-01/0329/240329.pdf

• Cyber Security and Resilience Bill: policy statement (Department for Science, Innovation and Technology, April 2025) – https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement

• NCSC blog on the Cyber Security & Resilience Bill policy statement – https://www.ncsc.gov.uk/pdfs/blog-post/cyber-security-resilience-bill-policy-statement.pdf

• House of Commons Library briefing (Dec 17, 2025) – https://commonslibrary.parliament.uk/research-briefings/cbp-10442/

Letter of Submission

The Cyber Scheme
Floor 7, Eagle Tower
Montpellier Drive
Cheltenham GL50 1TA

Date: 20 January 2026

To: The Chair, Public Bill Committee
Cyber Security and Resilience (Network and Information Systems) Bill

Dear Chair,

I am writing to submit a set of targeted amendments that embed professional assurance for cyber security roles by referencing the professional titles of the UK Cyber Security Council (UK CSC). These insertions use consistent “have regard to” language at points in the Bill where regulated entities rely on workforce competence to discharge statutory duties, such as risk management, incident response, designation as critical suppliers, and compliance assessments.

Our objective is to support proportional regulation that recognises diverse organisational contexts while providing regulators and operators with a clear, recognised benchmark for cyber professionalism. This approach aligns with the Department for Science, Innovation and Technology’s policy statement and the National Cyber Security Centre’s focus on closing capability gaps across critical sectors. It also complements existing frameworks (including the Cyber Assessment Framework) without mandating a single certification route.

We have ordered the amendments by clause for ease of consideration and included short explanations for each. We would welcome the Committee’s consideration of these proposals and stand ready to assist with drafting refinements, line references, and sector-specific tailoring through codes of practice and secondary legislation.

Yours faithfully,

Zeshan Sattar
Commercial Director

Proposed Amendments

Amendment – Duties of relevant digital service providers

Clause 8, page 7, line 36, after subsection (2A), insert –

(2B) Where measures adopted under subsection (1) concern the performance of workforce roles and the qualifications of personnel responsible for cyber security, those measures must be made with regard to the appropriate professional titles of the UK Cyber Security Council.

Explanation

Clause 8 sets core duties for Relevant Digital Service Providers (RDSPs) i.e. online marketplaces, search engines, cloud. Aligning staff competence with UK CSC professional titles provides recognised assurance for RDSPs' cyber workforce and supports proportionate regulator oversight.

Amendment – Duties of managed service providers to manage risks

Clause 10, page 9, line 25, after subsection (2), insert –

(2A) In carrying out the duties under this regulation, a relevant managed service provider must ensure that activities relating to the management of risks to network and information systems are undertaken by cyber security personnel whose competence is demonstrated with regard to the appropriate professional titles of the UK Cyber Security Council.

Explanation

MSPs hold privileged access to customers' systems. Requiring risk management functions to be staffed by UK CSC–titled professionals strengthens assurance for customers and regulators and is proportionate to the access and responsibility MSPs hold.

Amendment – Digital or managed service providers: meaning of "subject to public authority oversight"

Clause 11, page 10, line 3, at end, insert –

(x) In determining whether a provider that is subject to public authority oversight nonetheless derives more than half of its income from activities of a commercial nature, the provider must, where relevant, demonstrate that cyber security functions are performed by personnel with regard to the appropriate professional titles of the UK Cyber Security Council.

Explanation

Clause 11 determines scope for mixed public/commercial providers. Referencing UK CSC titles offers a consistent indicator of professional assurance when regulators assess borderline cases.

Amendment – Critical Suppliers

Clause 12, page 10, line 15, after provisions enabling designation (page 12, line 17), insert –

(X) In determining whether to designate, review, or remove a designation of a person as a critical supplier, the competent authority must have regard to whether the person ensures that cyber security functions are performed by personnel holding, or working towards, appropriate professional titles of the UK Cyber Security Council.

Explanation
Critical suppliers sit deep in essential service supply chains. UK CSC titles provide an auditable benchmark for competence that aids proportional decisions on designation and ongoing assurance without creating a hard credential mandate. Working towards an appropriate professional title could be demonstrated by holding the broad Associate (ACSP) title.

Amendment – Reporting of incidents by regulated persons

Clause 15, page 22, line 41, after 'In this regulation and regulations 11A and 11B, "regulated person" means an OES, an RDSP, an RMSP or a critical supplier,' insert –

(10) A regulated person must ensure that incident triage, containment, and post-incident review are led by cyber security personnel whose competence is demonstrated with regard to the appropriate professional titles of the UK Cyber Security Council.

Explanation
Incident response quality materially affects harm and learning. Referencing UK CSC titles for those leading triage and post-incident reviews strengthens the reliability of reporting and lessons learned across regulated sectors.

Amendment – Notification of Incidents to Customers

Clause 16 (Notification of incidents to customers), at end, insert –

(X) Where a regulated person is required to notify customers of an incident, the regulated person must ensure that the assessment informing the notification is reviewed by cyber security personnel whose competence is demonstrated with regard to the appropriate professional titles of the UK Cyber Security Council.

Explanation
Customer notifications depend on accuracy and proportionality. A UK CSC–titled reviewer adds a defensible competence layer to these determinations, especially for MSPs and RDSPs.

Amendment – Guidance Issued under the NIS Regulations

Clause 19 (Guidance), after subsection (1), insert –

(1A) Guidance issued under this regulation may include guidance about the use of cyber security personnel holding professional titles of the UK Cyber Security Council, and relevant regulatory authorities must have regard to such guidance when exercising their functions under the NIS Regulations.

Explanation
Clause 19 empowers guidance that drives consistent practice. Signposting UK CSC titles within official guidance helps align sectors and reduces ambiguity when regulators assess "appropriate" competence.

Amendment – Regulations Relating to Security and Resilience of Systems

Clause 29 (Regulations relating to security and resilience of network and information systems), at end, insert –

(X) Regulations made under this section may include provision requiring persons regulated by the NIS Regulations to ensure that specified functions are undertaken by cyber security personnel whose

competence is demonstrated with regard to the appropriate professional titles of the UK Cyber Security Council.

Explanation
This creates a clear enabling power so that, where needed, future secondary legislation can specify functions for which UK CSC–titled personnel are expected—allowing flexibility as the threat and labour market evolve.

Amendment – Imposition of requirements on regulated persons

Clause 30, page 55, line 37, at end insert –

(6A) Where requirements imposed by virtue of subsection (1) concern workforce roles and qualifications of cyber security personnel, those requirements must be made with regard to the appropriate professional titles of the UK Cyber Security Council.

Explanation
Aligns any requirements imposed under Clause 30 with the UK cyber professional architecture, ensuring competence expectations are consistently benchmarked.

Amendment – Regulatory Authorities: Compliance Assessment Lens

Clause 31, page 56, line 30 (Functions of regulatory authorities: enforcement, sanctions and appeals), after conditions requiring a person exercising the power, at end insert –

(4C) to hold, or working towards, appropriate professional titles of the UK Cyber Security Council.

Explanation
Ensures inspectors from the regulators that are exercising this power have or working towards appropriate UK CSC titles which would support consistent expectations across sectors.

Amendment – Code of Practice

Clause 36, page 61, line 4 (Code of practice), after subsection (1), insert –

(1A) A code of practice issued under this section may, among other things, set out expectations for the use of cyber security personnel holding appropriate professional titles of the UK Cyber Security Council for specific roles, functions, or activities.

Explanation
The code will be the practical engine of Part 3. Referencing UK CSC titles enables sector-specific tailoring (e.g., incident response leads, vulnerability management, SOC analysis) while remaining non-prescriptive.

Amendment – Inspections

Clause 47, page 72, line 9 (For the purposes of an inspection under subsection (2) or (3), the regulated person must), at end insert –

(8G) Where a regulated person appoints a liaison to facilitate inspections under this section, the regulated person must ensure that the liaison has appropriate competence with regard to the professional titles of the UK Cyber Security Council.

Explanation

When national-security-related directions are in play, competence of the inspection liaison is critical to timely, accurate cooperation. This keeps the “regard” threshold high without over-specifying roles.

January 2026

References

1. Cyber Security and Resilience (Network and Information Systems) Bill [Bill 329, as introduced]. Available at: https://publications.parliament.uk/pa/bills/cbill/59-01/0329/240329.pdf

2. Cyber Security and Resilience Bill: policy statement (DSIT, April 2025). Available at: https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement

3. NCSC blog on the Cyber Security & Resilience Bill policy statement. Available at: https://www.ncsc.gov.uk/pdfs/blog-post/cyber-security-resilience-bill-policy-statement.pdf

4. House of Commons Library briefing (Dec 17, 2025). Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-10442/