UK Finance

EVIDENCE TO THE PUBLIC BILL COMMITTEE

Cyber Security and Resilience (Network and Information Systems) Bill

Submitted by: UK Finance
Date: January 2026

About UK Finance

1. UK Finance is the collective voice for the banking and finance industry. Representing around 300 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation. Our members include large and small banks, building societies, asset managers, payment service providers and fintech firms operating in the UK.

2. The financial services sector is critical national infrastructure and already subject to comprehensive regulation on cybersecurity and operational resilience by the Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA). Our members invest significantly in meeting these regulatory obligations and maintaining the security and resilience of UK financial services.

Summary of Key Concerns

3. UK Finance supports the Government's objectives to strengthen national cyber resilience. However, we have significant concerns that the Bill, as currently drafted, may inadvertently capture already heavily regulated financial services firms through secondary provisions, creating regulatory duplication and undermining the coherent sectoral framework established by the financial services regulators.

4. This submission is informed by a roundtable meeting held on 3 December 2025, attended by over 110 member representatives, demonstrating the significant interest in this legislation across the sector. Our analysis, supported by external legal advice and engagement with HM Treasury and the PRA, identifies five areas where clarity or amendment is required.

Managed Service Provider Designation

5. The Bill's provisions on managed service providers (MSPs) lack clarity on whether existing financial services regulation would take precedence where FCA or PRA-regulated firms provide services to other regulated financial institutions.

6. UK Finance has identified scenarios where our members could be considered MSPs when providing financial services to other UK financial sector entities. Regulatory reporting

companies, which self-identify as fintech firms, expressed concern they could be unexpectedly captured by MSP designation despite already operating under FCA oversight.

7. **Intra-group concerns**: Where intragroup arrangements support Important Business Services, they are already subject to comprehensive regulatory oversight under the operational resilience regime (PS21/3), including requirements for resilience testing, mapping, and impact tolerances, making a MSP designation under this proposed legislation duplicative with possible conflictions. Where arrangements do not support IBS, both the providing and receiving entities remain PRA or FCA-regulated firms subject to supervisory oversight, governance requirements, and operational risk management frameworks, with regulators retaining powers to impose additional requirements where risks are identified. Subjecting services between regulated financial institutions to MSP designation under NIS would fragment regulatory accountability by introducing a parallel oversight regime for entities already within the regulatory perimeter of sectoral regulators with established supervisory relationships and sector-specific expertise.

8. **Recommendation**: The Bill should explicitly provide that an entity should not be subject to the relevant managed service provider (RMSP) definition where:

- The entity is subject to and regulated by applicable financial services law; or
- The entity is an intra-group company providing a managed service to an entity subject to and regulated by applicable financial services law **and** that entity is subject to the same group-wide ICT risk management framework that is intended to ensure compliance with relevant operational resilience requirements prescribed under financial services law.

Data Centre Capacity Thresholds

The Bill designates data centres above 10-megawatt capacity as operators of essential services. Several UK Finance members operate data centres at or above this threshold and would consequently fall within scope despite already being subject to stringent PRA and FCA regulation on operational resilience and critical operational infrastructure.

9. Critical drafting ambiguity: We have identified a fundamental uncertainty in how the 10MW threshold applies:

    - Does it apply per individual data centre?
    - If aggregated, this would be inappropriate as some capacity represents redundancy and resilience by design, not operational load.
    - It is not clear if the '*information technology services'* are required to be in the UK.

10. **Co-location arrangements**: We also raise concerns about shared data centre arrangements where facilities exceed 10MW but house multiple organisations. There is uncertainty whether obligations would extend to tenant firms or apply only to the data centre operator.

11. **Supervisory consolidation**: Under the Bill, any firm's data centres that *were* captured by the proposals would automatically be regulated by the Information Commissioner. In the context of financial services, sectoral regulators will have better sight of firms' operations and resiliency and security planning. We also note the Information Commissioner's recent statement, including concerns regarding resourcing this expanded mandate.

12. **Recommendation**: DSIT should confirm that the threshold applies per facility basis that recognises resilience architecture that supports the Bill's fundamental aims. Additionally, the Bill should explicitly exempt firms already regulated by the PRA, FCA or BoE from data centre provisions to prevent duplicative regulation and conflicting obligations, particularly where financial services firms rely on third-party providers for critical infrastructure. Finally, supervision of firms' data centre operations should defer to sectoral regulators where such supervisory relationships already exist.

Incident Reporting Requirements

13. The Bill imposes incident reporting obligations requiring initial reports within 24 hours and full reports within 72 hours. This adds to an already fragmented incident reporting landscape that UK Finance has consistently argued requires consolidation rather than expansion.

14. **Evidence of reporting proliferation**: UK Finance contends that internationally operating firms can already face approximately 150 incident regulatory reporting requirements following a global incident. Within a single year, the UK financial sector has faced multiple incident reporting regime change proposals including:

- PRA requirements under CP17/24
- FCA requirements under CP24/28
- Home Office ransomware proposals
- DSIT provisions under this Bill

15. **Additional complexity**: For firms with in-scope data centres, incident reporting would need to go to DSIT and Ofcom as designated competent authorities for that subsector, creating yet another reporting layer for organisations already navigating an exceptionally complicated environment.

16. **Recommendation**: Firms already regulated by the FCA, PRA and BoE should be explicitly carved out from incident reporting provisions under this Bill. Reporting should flow through established sectoral regulators who can coordinate with other authorities as necessary. Before introducing new reporting obligations, the Government should consolidate and simplify the existing fragmented regime.

Critical Supplier Designation

17. The Bill grants regulators and the ICO power to designate critical suppliers where supply chain disruptions could have significant economic or societal impact. This risks duplicating the Critical Third Parties (CTP) regime established specifically for financial services.

18. **Risk of double designation**: UK Finance is concerned that firms providing payment or other services already designated by the FS regulators under the CTP regime could find themselves additionally designated under this Bill, creating disproportionate and duplicative requirements for the same activities and unnecessarily increasing costs for service users. Additionally, there is further risk of duplication where firms have been designated as Critical National Infrastructure.

19. **Positive aspects acknowledged**: Our members welcomed aspects of critical supplier designation as additional levers to improve supplier software quality, noting that approximately 50% of incidents originate from the supply chain. However, this must not duplicate existing regulatory frameworks.

20. **Recommendation**: Amend the critical supplier designation provisions to require mandatory consultation with the FCA, PRA and BoE before designating any firm already regulated by those authorities. Where a firm is subject to equivalent requirements under financial services regulation, designation under this Bill should not proceed.

National Security Directives

21. The Bill grants the Secretary of State power to issue binding directives requiring entities to take necessary and proportionate action in response to imminent threats to national security. Whilst UK Finance recognises the importance of national security, we have concerns about how such powers would operate in practice.

22. **Operational constraints:** As an illustrative example of where this may manifest, systems forming part of global payment infrastructures require careful project planning for patch implementation and system changes. Legislation granting the Secretary of State power to requiring action on timescales that do not accommodate safe implementation and confident restoration of critical systems could create operational risks rather than mitigate them.

23. **Existing collaborative frameworks:** Within financial services, current arrangements already operate effectively. The financial sector collaborates on threat response through established channels built on trust, openness, and willingness to acknowledge issues without fear of penalties.

24. **Recommendation:** Before exercising national security directive powers over regulated financial services firms or their critical suppliers, the Secretary of State should be required to consult with the Bank of England, PRA, and FCA to ensure directives are operationally feasible and do not conflict with financial stability or prudential requirements. This consultation requirement should apply consistently across all regulated sectors, with the Secretary of State engaging relevant sectoral regulators before issuing directives that could impact regulated entities or their supply chains. Any timescales imposed must accommodate the safe implementation requirements of critical payment and financial infrastructure.

Overarching Recommendation

25. The fundamental issue underlying all five concerns is the risk of regulatory duplication and incoherence. The financial services sector is already subject to vigorous cybersecurity and operational resilience regulation specifically designed for the unique characteristics and systemic importance of financial services.

26. **Recommendation**: We recommend the Bill include an explicit provision establishing that where firms are regulated by the FCA, PRA and BoE, the requirements of financial services regulation take precedence with firms exempt from provisions under this Bill. This approach mirrors the EU framework where DORA takes precedence over NIS2 for financial entities (DORA Article 4).

27. This would achieve the Government's stated objective of avoiding regulatory duplication, maintain the coherent sectoral approach developed by financial services regulators, and ensure the sector continues to meet robust cybersecurity standards without the burden and confusion of overlapping requirements.

28. Beyond concerns about regulatory duplication, UK Finance emphasises the significant risk of conflicting regulatory outcomes between financial services regulators and DSIT/ICO under this Bill. Where different regulators impose divergent requirements on the same

activities, firms face very difficult compliance choices that could undermine both financial stability and cyber resilience objectives.

29. We remain committed to engaging constructively with the Government and stand ready to provide further evidence or technical expertise to the Committee as required.

Contact:
Adam Avards
UK Finance
adam.avards@ukfinance.org.uk