Cyber Security and Resilience (Network and Information Systems) Bill

Bill 329 2024-26

Written Evidence Submitted by iProov 29th January 2026

1. Executive Summary

1.1. This submission provides comments from iProov on the Cyber Security and Resilience (Network and Information Systems) Bill 2025, specifically addressing the systemic risks associated with digital identity in the United Kingdom's infrastructure.

1.2. The UK faces cascading risks driven by geopolitical tensions and rapid technological shifts.Within this framework, identity has emerged as the most critical point of failure. The inability to verify digital identity with high assurance enables both massive economic fraud and adversarial state espionage.

1.3. Current cybersecurity paradigms focus on hardening assets, yet 57% of UK Critical National Infrastructure (CNI) organisations reported a supply chain attack in the past year. Vulnerability now resides in the interconnections of systems, including API calls, supply chain links, and human-system interfaces, where identity is the primary gatekeeper.

1.4. The evidence suggests that high-assurance digital identity verification must be formally designated as CNI. We identify opportunities within Clauses 12 and 30 of the Bill to integrate identity resilience into the UK's statutory framework, ensuring that the identity layer receives commensurate oversight and intelligence support.

2. The Strategic Context and Identity Vulnerability

2.1. The stability of the UK's essential services is under unprecedented pressure. Geopolitical conflicts, such as the ongoing war in Ukraine, have directly increased the volume of cyberattacks targeting UK infrastructure. These attacks increasingly utilise weaponised artificial intelligence (AI) to bypass traditional security perimeters.

2.2. The economic impact of identity-related failure is quantifiable and escalating. In 2024, UK payment fraud losses reached £1.17 billion, with identity fraud accounting for 59% of all cases in the National Fraud Database. The annual cost of identity fraud to the UK economy is estimated at £1.8 billion.

2.3. Of particular concern is Synthetic Identity Fraud (SIF), which is the creation of fictitious synthetic identities using a blend of real and fabricated data. SIF is projected to cost the UK economy £4.2 billion by 2027 if unaddressed. Furthermore, money mule networks, facilitated by weak liveness verification, launder an estimated £10 billion annually through the UK financial system.

2.4. These economic threats are mirrored by national security risks. State-sponsored actors, including those from Russia, China, and North Korea, are documented using deepfakes and fabricated identities to secure access to sensitive IT environments and CNI systems.

3. Clause-by-Clause Review of the Bill

3.1. Part 2, Chapter 1: Regulated Persons (Clauses 4, 6, 9, and 10)

3.1.1. The Bill correctly expands the definition of essential services to include data centres (Clause 4) and large load controllers (Clause 6). However, the security of these physical and digital assets is fundamentally dependent on the identity of those accessing them. A data center is only as secure as the verification process for its privileged administrators.

3.1.2. Clause 9 brings Managed Service Providers (MSPs) into scope. Given that MSPs possess unprecedented access to customer systems, they are high-value targets for persistence techniques utilising legitimate tools. iProov recommends that the appropriate and proportionate measures mandated in Clause 10 must explicitly include high-assurance identity verification for any personnel with administrative access to CNI-linked networks.

3.2. Clause 12: The Critical Supplier Regime

3.2.1. Clause 12 allows regulators to designate third-party suppliers as critical if their disruption would significantly impact the economy or society. This represents the appropriate mechanism for recognising the foundational role of identity providers.

3.2.2. High-assurance digital identity providers function as a critical cross-cutting dependency across all 13 existing CNI sectors. If a nationally significant identity provider is compromised, the ability of the NHS to verify clinicians, or the ability of banks to prevent SIF, is immediately rendered inoperable. Designation under Clause 12 would allow these providers to receive direct NCSC intelligence support and rigorous regulatory oversight.

3.3. Clause 15: Incident Reporting

3.3.1. The Bill introduces a two-stage reporting model (24-hour initial, 72-hour full). Clause 15(2) expands reporting to incidents capable of having an adverse effect.

3.3.2. For identity providers, an incident capable of having an adverse effect includes the discovery of a significant new AI-driven injection methodology. iProov recommends that the reporting framework encourages the sharing of real-time threat intelligence regarding new deepfake typologies across regulated sectors.

3.4. Clause 30: Imposition of Requirements

3.4.1. Clause 30 provides the Secretary of State with broad powers to impose security requirements on regulated persons. This clause should be used to mandate minimum technical security baselines that are resilient against generative AI.

3.4.2. Current standards often rely on Presentation Attack Detection (PAD), which assesses physical spoofs like masks. However, modern adversaries have pivoted to Digital Injection Attacks, which bypass the camera sensor entirely. iProov's intelligence indicates a 300% surge in AI-driven injection attacks in 2024. Requirements under Clause 30 must prioritise proving a person is the right person, a real person, and authenticating in real-time using biometrics with advanced Liveness.

4. Technical Analysis: The Failure of PAD Standards

4.1. The current UK Digital Identity & Attributes Trust Framework (DIATF) is process-based and lacks the prescriptive technical controls found in international models like NIST SP 800-63-4 or eIDAS 2.0 (incorporating ETSI 119 461 and CEN TS 18099).

4.2. Existing PAD standards (ISO/IEC 30107-3) do not adequately address digital injection. A comparison of regulatory rigour is provided below:

Threat Vector	NIST SP 800-63-4 (US)	eIDAS 2.0 (EU)	UK DIATF (Current)
Presentation Attack	Prescriptive metrics (IAPAR <0.07)	Legally Mandated (Level: High)	Process-based audit
Digital Injection	Mandatory technical controls	Required for Highest Security	Addressed via general ISMS
AI-Generated Media	Mandatory artifact analysis	Explicit technical standards	Fraud audit requirement

4.3. Without a mandate for biometrics with advanced Liveness, the lower regulatory baseline in the UK means that UK DIATF certified providers remain vulnerable to scalable AI-driven impersonation. Malicious actors may view the UK as offering a lesser degree of defence against such attacks than either the EU or US.

5. Proposed Amendments to the Bill

Amendment 1: Designation of Identity Providers as Critical

Clause 12, Page 10, line 23, at the end insert-

"(ba) P provides high-assurance digital identity or biometric verification services

> relied upon by an OES for the purpose of securing access to essential services;"

Rationale: This ensures that identity providers are explicitly recognised as potential Critical Suppliers, allowing for CNI-equivalent oversight.

Amendment 2: Technical Resilience Requirements

Clause 30, Page 55, line 30, at the end insert-

> "(aa) requirements to implement identity verification measures that are resilient against digital injection and generative AI-driven impersonation;"

Rationale: This empowers the Secretary of State to mandate that appropriate measures must include defence against the 300% surge in AI-driven injection attacks.

Amendment 3: Code of Practice on Genuine Presence

Clause 36, Page 61, line 5:
Add at the end of paragraph (1):

> "The code of practice must include specific technical guidance on the detection of digital injection and the assurance of genuine presence in remote identity verification."

Rationale: This ensures that the Code of Practice reflects the modern threat landscape and provides a clear technical benchmark for regulated persons.

6. Conclusion

6.1. The Cyber Security and Resilience Bill is a necessary step to address the UK's systemic fragility. However, the Bill will only achieve its objectives if it addresses the foundational vulnerability of digital identity.

6.2. By designating high-assurance identity providers as Critical National Infrastructure and mandating resilience against AI-driven injection attacks, the UK can raise the defensive floor for the entire economy, protecting £4.2 billion in projected losses and safeguarding national security against state-sponsored and asymmetric threats.

For further information contact: Campbell.Cowie@iproov.com