**Further written evidence submitted by iProov (CSRB35)**

just an additional note to submit in evidence, as a complement to my earlier submission (from iProov). We are deeply focussed on similar debates regarding the threat to CNI due to vulnerabilities in the identity systems securing online and physical access in other Five Eyes countries. Therefore, we have compiled the attached advisory note detailing the baseline technical requirements for identity verification and authentication solutions employed in the protection of CNI and the key 3rd party/value chain operations. I would like to see this considered alongside discussion on Clause 36 of the Cyber Security and Resilience Bill, which concerns the issuance of Codes of Practice by the Secretary of State.

**Proposed Text:** Clause 36, Page 61, line 5, add at the end of paragraph (1):

*"The code of practice must include specific technical guidance on detecting digital injection and assuring genuine presence in remote identity verification."*

I would respectfully invite the Committee to consider the suitability of there being a technical baseline along the lines of that attached. Very happy to discuss or provide additional information if it would be appropriate.

Thanks,

Campbell Cowie

**Recommended Technical Baseline for High-Assurance Identity Resilience in UK Critical National Infrastructure- iProov**
V2.2
4nd February 2026

**Introduction**

Biometric identity verification services are used to confirm the identity of a remote user, in an untrusted context, using an untrusted hardware and software environment, and an untrusted network connection. This document addresses specifically Liveness performance, which is the most security-critical element of such verification. The extent of protection required depends on a threat analysis for the use case. For mission-critical use cases where the compromise of access leads to systemic risk to essential services, the following criteria represent an evidence-based baseline for achieving technical resilience against generative AI-driven threats. Alternatively, if it is highly likely that a successful attack on the remote biometric identity verification will be consistently detected and blocked by another measure, preventing serious consequences in all cases albeit at higher operational cost, then some of these requirements may be relaxed.

## Inclusion

1. **Certified compliance with WCAG 2.2 AA**

   Necessary to ensure adequately wide inclusion of citizens, including those with disabilities.

2. **Demonstrably low false reject rates (<5% average) across the full range of devices citizens or staff might reasonably be expected to use.**

   Necessary to ensure no discrimination on the basis of economic ability to buy mobile devices and inclusion of those who can afford only low-cost devices, of which there is a very large variety.

   Evidence should be required to demonstrate such performance on all iPhones with iOS15 and above, and on >10,000 Android mobile devices, including devices running Android 8 and above, measured on >100,000 attempts. This is necessary to deliver statistically significant evidence across the full range of applicable devices.

   Measurements should be demonstrably from in-field service, without any service-provider human intervention.

3. **False reject rates not vary by >0.5% between ethnicities, genders and ages, with mandatory regular reporting**

   Measured in in-field service, necessary to ensure no significant discrimination against any societal group and ensure full social inclusion. A demonstrable program to ensure continued compliance is required, including the provision to HMG of regular equality of outcome reports.

## Best Practice compliance

Certification by a UKAS (or equivalent)-approved Conformity Assessment Body (CAB) or test laboratory (TL) (as applicable) against:

1. **FIDO Face Verification Certification (TL)**

   This is the only independent, international certification test standard for the performance of biometric face verification and liveness, intended to set an adequate standard for “selfie match” performance during identity setup.

2. **ETSI 119-461 v2.1.1 (2025-02) Certification (CAB)**

   The EU standard for remote identity verification, incorporating CEN/TS 18099:2025: the standards for the EU Digital Identity Wallet.

   Testing laboratory (**TL**) test results must be provided against CEN/TS 18099:2025 to demonstrate a high level of assurance for Injection Attack Detection. Each TL has its own scale of assurance. A risk-appropriate requirement is provided by Ingenium Laboratories Assurance Level 4.

3. **GBG 44 Level Very High & GBG 45 Score 3 compliance (CAB)**

   Relevant Certifications to GBG 44 and GBG 45 should be required as a baseline. GBG 44 Very High should be achieved when used as part of a multi-factor authentication solution. GBG 45 Score 3 is the highest level achievable by a remote biometric capture solution reliant on the user’s own device and should be mandatory. These certifications do not meet the requirements of eIDAS 2.0 Level of Assurance High, which should therefore be treated as an additional requirement (see below).

## UK Economic Advantage

1. **Independently audited compliance with EU standards ETSI 119-461 v2.1.1, CEN TS18099 and eIDAS 2.0 (EU910/2014 as amended by EU2024/1183) Article 24.3**

   Providers must demonstrate a clear roadmap for maintaining alignment with evolving eIDAS 2.0 technical specifications for the EU Digital Identity Wallet to ensure future-proofed interoperability. Although recognising ETSI and CEN standards, the UK is not bound by them nor by the eIDAS Regulation. Maintaining technical alignment with leading international benchmarks (such as eIDAS 2.0 and CEN/TS 18099) ensures the UK remains a leading global cyber innovator. This interoperability ensures UK credentials remain portable for digital trade, directly supporting the government's 'Tech for Growth' mission.

## Security Requirements

1. **Cloud Security Alliance (CSA) Star**

   The current international standard for the cyber-security of cloud-based services, to assure the security resilience of any service supplied to HMG.

2. **Cyber Essentials certification**

   Necessary to ensure alignment with HMG cyber security policy under PPN014.

3. **Hybrid automatic/manual cloud-based biometric fraud monitoring & detection**

   To secure against evolving AI threats, the provider must actively monitor and risk-assess all verification attempts. High-risk transactions must undergo analysis by examiners with a high level of technical expertise capable of identifying linked threats within the entire system traffic, to identify and rapidly respond to emerging threats. The service must be capable of implementing updates 30 times per month, while limiting the administrative load on [HMG Department] to a maximum of one update per quarter.

4. **Visibility of, and data from, threats in Latin America, APAC and the United States as well as the UK**

   Threats to UK infrastructure come from around the world and may be developed and tested in other regions before being unleashed on the UK. The speed with which such threats evolve may not give the UK sufficient time to respond if visibility is limited just to the UK or the EU. Therefore any provider must have direct, ongoing access to threat data and intelligence from field operations and experience of mitigating such threats with high-value targets, including governments, in multiple regions of the world which are subject to high threat intensity.

5. **Attack Presentation Classification Error Rate (APCER) (ISO 30107-3)**

   APCER (or where tested, IAPAR) as measured by a UKAS certified laboratory must not exceed 0.01%, at a system FRR of <5% measured over >5,000 attempts, to deliver an acceptable minimum level of protection to HMG.

6. **Injection Attack Detection independent tested >Level High (CEN 18099)**

   The system must exceed CEN High performance or a reasonable equivalent through testing under an evaluation scheme that is conformant to CEN 18099 or an equivalent and involves a minimum of 40 days testing by an ISO 17025-accredited test laboratory. An example would be Ingenium Laboratories Level 4.

7. **UK Hosted processing**

   All normal processing functions, automated and manual, must take place in the United Kingdom.  Manual review of potentially fraudulent transactions may also take place within the EU.

8. **Software and service supply chain transparency via SBOM**

   No part of the supply chain for software or service delivery may include entities or personnel who are or have previously been owned by or employed by state entities in countries currently subject to UK sanction. Suppliers must provide a comprehensive Software Bill of Materials (SBOM) to verify the provenance of all critical components.

## Throughput & Scaling Requirements

1. **Throughput**

   The system must be able to support loads of up to [*use-case dependent*] transactions per second at peak times

2. **Scaling**

   Details of the system's method of scaling (horizontal vs vertical) and total cost of ownership, including estimates of any consequential processor costs likely to be incurred by [*HMG Department*] for different scales, should be provided.

## Record of Success in Delivery of Government Projects

1. **Track record of best practice partnerships with UK Government**

   Suppliers must be able to demonstrate success in delivery of its service in the context of high-profile UK citizen-facing identity solutions in the public sector, where each is widely recognised as representing best practice.

2. **UK supplier with an international reputation for critical infrastructure projects**

   To mitigate the delivery risk of a critical service, the supplier must be able to demonstrate an international reputation for successfully protecting critical infrastructure. To mitigate vulnerability to international political uncertainties affecting critical supply chains, preference should be given to providers demonstrating sovereign capability, including UK-based R&D and significant processing footprints within the United Kingdom. Such risk mitigations will help meet the concerns of the press and those tasked with political oversight.