iProov's Response to Proposed Amendments to the Critical Infrastructure Risk Management Program (CIRMP) Rules

9th February 2026

1. Executive Summary

iProov welcomes the opportunity to provide this submission to the Department of Home Affairs regarding the proposed amendments to the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (the CIRMP Rules).

iProov is a leading provider of high-assurance digital identity solutions, including the biometric liveness technology that underpins the Australian Government's myID (formerly myGovID) and Singapore's Singpass national identity programs. This submission draws on our international experience in securing sovereign digital ecosystems to address the evolving threat facing Australia's critical infrastructure.

Australia faces a complex security environment characterised by the convergence of geopolitical tensions, economic instability, and rapid technological shifts, including generative artificial intelligence (AI). The Hon Tony Burke MP, Minister for Home Affairs and Cyber Security explicitly linked the convergence of geopolitical tensions and advanced technology in his address for the release of the *Critical Infrastructure Annual Risk Review 2025*.

> *"The latest Critical Infrastructure Annual Risk Review highlights the changing risk landscape faced by Australia's critical infrastructure... [including] the emergence of new and more complex risks from agentic artificial intelligence and other cutting-edge technology, persistent risks of sabotage as well as skill and staffing shortages... occurring alongside unpredictable changes in the global geopolitical environment."* [1]

Consequently, the resilience of critical infrastructure faces distinct and escalating pressures. Intelligence from the Australian Signals Directorate (ASD) and the Australian Security Intelligence Organisation (ASIO) confirms that state-sponsored actors, such as Volt Typhoon, are actively mapping and targeting critical networks to gain strategic leverage. Mike Burgess, Director-General of Security (ASIO), in his 2025 Annual Threat Assessment aptly characterises the convergence of threats.

> *"The future... is one that is under pressure from great-power competition, the diffuse post-Covid-19 constellation of anti-authority grievances and ever-mutating radicalisation pathways, all accelerated by technological advances... establishing security priorities at a strategic level [will be] far more difficult."* [2]

---

[1] The Hon Tony Burke MP (Minister for Home Affairs and Cyber Security), *Critical Infrastructure Annual Risk Review 2025*:
https://www.tonyburke.com.au/media-releases/2025/critical-infrastructure-annual-risk-review-highlights-changing-risk-landscape

[2] Mike Burgess (Director-General of Security), *Annual Threat Assessment 2025*:

iProov's core position is that high-assurance digital identity verification is the root of trust for the cyber, personnel, and supply chain security of every critical asset in Australia. To address the contemporary threat profile, this submission argues for:

1. **Formal Recognition of Identity as CNI:** Nationally significant identity providers should be designated as critical infrastructure assets under the *Security of Critical Infrastructure Act 2018* (SOCI Act).
2. **Mandating Advanced Liveness Detection:** The CIRMP Rules must mandate technical standards for Injection Attack Detection (IAD) to mitigate the 300% surge in AI-driven digital injection attacks.
3. **Strengthening Phishing-Resistance:** Defining phishing-resistant MFA in the Cyber 3 measure to include un-replayable biometrics.[3]

2. Identity as a Foundational Vulnerability

Current threat intelligence indicates a shift in the critical point of failure from individual assets to the interconnections within systems, in particular API calls, supply chain links, and human-system interfaces.[4] Identity is the primary gatekeeper for these interconnections.

The economic and operational consequences of security failures are material. Modelling indicates that a single espionage-enabled cyber incident affecting critical infrastructure can cost more than $1 billion.[5] Domestically, identity fraud is the most common cybercrime reported by Australians, representing 30% of total reports in the last financial year.[6] Furthermore, the Australian Federal Police estimates identity crime costs the national economy over $5.6 billion annually.[7] For large businesses, losses from identity-related cyber incidents surged by 219% in a single year, highlighting the industrialisation of credential theft by malicious actors.[8] High-assurance identity verification acts as a strategic imperative to neutralise these vectors by securing IT/OT boundaries and preventing credential theft.

---

https://www.oni.gov.au/news/asio-annual-threat-assessment-2025

[3] SOCI Act 2018 IAM Obligations for Critical Infrastructure - RSA Security. https://www.rsa.com/resources/blog/zero-trust/soci-act-2018-iam-obligations-for-critical-infrastructure/

[4] See Australian Signals Directorate (ASD), *Annual Cyber Threat Report 2024–2025* (Report, October 2025) p. 28, noting that malicious actors increasingly exploit vulnerabilities in third-party supply chains and interconnected edge devices https://www.cyber.gov.au/sites/default/files/2025-10/Annual%20Cyber%20Threat%20Report%202024-25.pdf.

[5] Australian Institute of Criminology (AIC), *The Cost of Espionage* (Report, July 2025), https://www.aic.gov.au/publications/special/special-21

[6] Australian Signals Directorate (ASD), *Annual Cyber Threat Report 2024–2025* (Report, October 2025). https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025

[7] Australian Federal Police (AFP), *Cost of Identity Fraud in Australia* (Estimate, 2022/2025). https://www.aic.gov.au/sites/default/files/2025-08/sr53_cybercrime_in_australia_2024_v2.pdf

[8] Australian Signals Directorate (ASD), *Annual Cyber Threat Report 2024–2025* (Report, October 2025). https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025

3. Response to Policy Design Questions

Cyber and Information Security Hazard Measures

Cyber 1: Cyber security framework uplift - iProov supports the uplift to Maturity Level 2 for high-risk asset classes. However, we note that framework compliance is only effective if the identity layer is secured to a High Level of Assurance (consistent with IAL3 under NIST SP 800-63-4 or eIDAS 2.0). For entities with an operational technology (OT) component, identity binding must be the first step in protecting the system from lateral movement.

Cyber 2: Critical systems network protection - Architectural segregation between IT and OT networks is a fundamental architectural requirement. iProov recommends that the greatest practical level of segregation include mandated high-assurance identity verification for any personnel or automated system attempting to cross network boundaries. Identity verification should be a mandatory checkpoint for logical access between segregated systems.

Cyber 3: Multi-factor authentication (MFA) - The Department's focus on phishing-resistant MFA is critical, as compromised credentials remain a top-three incident type. However, traditional MFA is increasingly bypassed through AI-driven social engineering and session hijacking. While FIDO2/WebAuthn hardware tokens provide robust resistance against credential relay attacks, they verify only *possession* of the device, not the identity of the operator. In the context of Critical Infrastructure, where coercion and insider threats are material risks, this is insufficient.

The Australian Signals Directorate (ASD) has observed that generative AI is significantly lowering the technical barrier for such attacks, enabling malicious actors to scale sophisticated impersonation and credential theft at an unprecedented rate. [9]

- **Recommendation:** The CIRMP Rules should explicitly define phishing-resistant for critical infrastructure to include biometrics that provide proof of genuine presence, thereby verifying the user's identity, liveness, and session authenticity.

Personnel and Supply Chain Hazard Measures

Personnel 2: Strengthened background checking - iProov supports the mandate for AusCheck background checks for critical workers. We note, however, that the integrity of any background check relies on the initial binding of a digital identity to a verified physical individual.

- **Opportunity:** High-assurance remote biometric verification should be encouraged to guarantee that even offshore or remote critical workers are the legitimate holders of their credentials, preventing the use of fabricated or synthetic identities by state-sponsored actors.[10]

---

[9] Australian Signals Directorate (ASD), *Annual Cyber Threat Report 2024–2025* (Report, October 2025). https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025

[10] Warnings of state-sponsored actors utilising generative AI to create fabricated personas and fraudulent KYC documentation to infiltrate sensitive networks are included in the Australian Signals Directorate (ASD), *Annual Cyber Threat Report 2024–2025* (Report, October 2025). https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-202

Supply Chain 2: Vendors of concern - Foreign ownership, control, and influence (FOCI) risks are particularly acute in the biometric and identity domain.[11]

- **Recommendation:** Responsible entities should be required to assess the data sovereignty and jurisdictional control of their identity providers. Dependence on identity providers influenced by hostile jurisdictions creates a strategic vulnerability where the authentication layer itself could be manipulated.

4. Alignment with Global Best Practice

This table maps identity-related threat vectors to controls commonly relied upon under current CIRMP-aligned practices, identifies observed limitations, and indicates potential control uplifts. Each threat is cross-referenced to the relevant cyber security obligations under the Critical Infrastructure Risk Management Program (Cyber 1-Cyber 3) to support the Department's assessment of regulatory coverage.

Threat Vector	Legacy Control (Current CIRMP)	Vulnerability	Recommended Uplift (Proposed CIRMP)	Relevant Standard	Relevant CIRMP Cyber Obligation
Presentation Attack (Masks, Photos)	ISO/IEC 30107-3 (PAD)	Assumes trusted camera hardware.	Active Liveness with depth/texture analysis.	ISO/IEC 30107-3 Level 2	Cyber 2 (Controls to mitigate material cyber risks)
Injection Attack (Virtual Camera, Emulator)	None / Generic Anti-Virus	Bypasses camera sensor entirely; scalable via AI.	Injection Attack Detection (IAD) with cryptographic binding.	CEN/TS 18099, NIST SP 800-63-4	Cyber 2; Cyber 3 (System security and integrity)
GenAI Deepfakes (Real-time Face Swap)	Passive Liveness	High-quality deepfakes can fool passive analysis.	Challenge-Response (e.g. Optical or Gestural) verifying real-time physics.	CEN/TS 18099	Cyber 2
Coerced User / Insider	FIDO2 / Hardware Token	Token validates, but the user is compromised.	Biometric Binding to the specific session.	NIST IAL3 / AAL3	Cyber 1 (Risk identification); Cyber 2
Foreign Interference (FOCI)	Generic Vendor Assessment	Biometric data stored in hostile jurisdictions.	Data Sovereignty Mandate for Identity Data.	SOCI Act (Supply Chain)	Cyber 1; Cyber 3

4-2025

[11] See Jason Van der Schyff, James Corera, and Justin Bassi, *In whose tech we trust: Mitigating foreign owned, controlled or influenced technology risks and building resilience* (ASPI Report, November 2025), which highlights the systemic vulnerabilities created when national systems depend on foreign vendors subject to external direction or legal obligations. https://www.aspi.org.au/report/in-whose-tech-we-trust-part-ii/

The threat and control mapping above demonstrates that identity-related attack vectors intersect with multiple cyber security obligations under the CIRMP Rules, rather than aligning to a single obligation. Cyber Security Obligation 1 (Cyber 1) is primarily engaged at the risk identification and assessment stage, particularly in relation to coercion risks, insider compromise, and foreign interference affecting identity systems and biometric data supply chains. These threats inform an entity's understanding of material cyber risks and dependencies relevant to critical assets.

Cyber Security Obligation 2 (Cyber 2) is engaged where entities implement and maintain controls to mitigate those identified risks. In this context, identity-centric threats such as presentation attacks, injection attacks and GenAI-enabled deepfakes represent vectors that may not be fully mitigated by controls traditionally focused on credentials, tokens or network-level protections. The indicative uplifts referenced in the table illustrate how controls aligned to recognised standards may be applied proportionately to address these risks.

Cyber Security Obligation 3 (Cyber 3) is engaged where the integrity, availability and confidentiality of systems supporting critical infrastructure may be undermined by compromise of identity verification mechanisms or upstream service providers. Injection attacks and supply-chain exposure affecting identity and biometric services have the potential to impact system security at scale and therefore intersect with obligations relating to system security, resilience and trusted operation.

This cross-walk is intended to assist the Department in assessing whether current CIRMP settings sufficiently capture identity-related cyber risks, and whether clarification or refinement may be warranted for high-risk asset classes or high-impact use cases.

References to CEN TS 18099 and NIST SP 800-63-4 reflect IDAS2.0 in the EU and the published Digital Identity Guidelines in the US, which include explicit consideration of forged, injected and synthetic identity artefacts within identity proofing and authentication processes. These references are provided for alignment purposes, noting Australia's established practice of harmonising cyber and identity controls with internationally recognised standards.

5. Addressing the Technical Gap: PAD vs. IAD

A significant risk in the proposed rules is the reliance on legacy security standards. Existing standards (ISO/IEC 30107-3) focus on Presentation Attack Detection (PAD), detecting physical spoofs like masks or photos.

Adversaries have now pivoted to Digital Injection Attacks, which bypass the camera sensor to feed synthetic media (deepfakes) directly into the system. These attacks surged by 300% in 2024.[12]

To ensure the CIRMP Rules remain effective against emerging threats at the time of

[12] https://www.iproov.com/reports/threat-intelligence-report-2025-remote-identity-attack

implementation, iProov recommends the Department mandate technical baselines that include Injection Attack Detection (IAD). This involves un-replayable biometric technology, such as controlled illumination (other approaches are available), to provide cryptographic proof of real-time authentication. We recommend the Rules specify that biometric controls for high-risk assets must be tested against CEN/TS 18099:2024 (Biometric data injection attack detection).

6. Strategic Recommendations for the Final Rule Design

Beyond the specific measures, iProov suggests the following enhancements to the CIRMP framework:

1. **Formal CNI Designation:** Nationally significant identity providers function as a critical cross-cutting dependency for all 13 asset classes listed in Table 1 of the Consultation Paper. Disruption of these providers would render clinicians, energy grid administrators, and transport operators unable to authenticate. They should be formally designated as CNI to receive direct intelligence and oversight. Rather than creating a new asset class, iProov recommends that the Department clarify the definition of Critical Data Storage or Processing Assets to explicitly include Identity and Access Management (IAM) and Biometric Verification providers that service critical infrastructure entities.This clarification would ensure that the supply chain dependencies of the identity layer are subject to SOCI Act oversight (particularly regarding FOCI and data sovereignty) without duplicating the accreditation functions of the Digital ID Act 2024. This approach harmonises the two legislative frameworks
2. **Harmonisation with International Standards:** Australia should align its technical requirements with the prescriptive models of NIST SP 800-63-4 (US) and eIDAS 2.0 (EU), which explicitly mandate controls against virtual cameras and device emulators.
3. **Dynamic Risk Advice:** The proposed Specified Risk Advice (All-hazard 1) should be used to provide rapid updates on emerging AI-driven identity deception typologies, compelling industry is mandated to implement timely technical mitigations.

7. Regulatory Impact Analysis

To support the Department, we have summarised publicly available market data to estimate the potential costs of the implementation.Commercial Off-The-Shelf solutions for IAD are mature (TRL 9), so a 12-18 month implementation window is realistic. This aligns with the Cyber 1 uplift timeline proposed in the consultation (compliance by 2028).

Estimated Costs: The implementation of cloud-based high-assurance identity verification is primarily an operational expense (SaaS). Current market rates for NIST IAL3-compliant biometric verification range from $1.00 to $3.00 per transaction. For a typical Critical Infrastructure entity managing 5,000 privileged users with monthly verification requirements, the annual cost is estimated at approximately $150,000 - $200,000.

Benefit Analysis: This cost is negligible (approx. 3.7%) when compared to the $4.03 million average cost of a data breach in Australia. Furthermore, it directly mitigates the >$1 billion economic risk associated with state-sponsored espionage incidents involving credential theft.

8. Conclusion

The proposed CIRMP amendments represent a significant advancement in Australia's national resilience frameworks. However, the security of Australia's critical infrastructure is only as robust as the identity layer that governs access to it. By mandating high-assurance liveness detection utilising genuine presence technology and recognising identity verification as a critical asset, the Government can safeguard Australian essential services against both criminal fraud and state-sponsored sabotage.

iProov remains committed to supporting the Department in the technical co-design of these standards.

Contact: Campbell Cowie Head of Policy, iProov ([redacted])