CLEARD LIFE VETTING AGENCY

Submission to the Exposure Draft of the Enhanced Critical Infrastructure Risk Management Program (CIRMP) Rules

Response to the Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026

Submitted by: Cleard Life Vetting Agency

Contact: Edward Barker, Director

Date: 31 March 2026

Scope: Personnel Hazards (Section 9A), Suitability Assessment, Offshore Critical Workers, and the role of AS 4811:2022

Classification: Public submission

1. Introduction and Standing

Cleard Life Vetting Agency is an Australian specialist provider of workforce screening, personnel security vetting, and security clearance management services. We are the first organisation in Australia to achieve auditor-certified conformance to all 19 mandatory and all 73 recommended clauses of the Australian Standard AS 4811:2022 *Workforce Screening*. We have served on the AGSVA panel and have processed national security clearances for over a decade across Defence, critical infrastructure, aerospace, and cyber security sectors. We currently manage a large AGSVA clearance portfolio for DISP members and aspiring DISP members, and provide our own Critical Infrastructure Clearance product—a suitability assessment conducted to AS 4811:2022—which is distinct from both AGSVA national security clearances and AusCheck background checks.

Cleard Life submitted to the initial Consultation Paper in February 2026 and that submission was published on the Department's website alongside those of the Business Council of Australia, CrowdStrike, Woodside Energy, and other major stakeholders. This submission responds to the Exposure Draft of the Enhanced CIRMP Rules released on 30 March 2026.

Our submission focuses on the personnel hazard provisions in section 9A of the Exposure Draft, with particular attention to three issues: (a) the absence of a recognised suitability assessment framework equivalent to those prescribed for cyber security, (b) the gap between AusCheck background checking and the insider threat risks the Rules seek to address, and (c) the practical challenge of assessing offshore critical workers who access Australian critical infrastructure systems.

2. Core Position: AS 4811:2022 as the Personnel Security Framework

The Exposure Draft prescribes specific, named frameworks for the cyber and information security hazard domain. Section 8A(3) lists five frameworks—AS ISO/IEC 27001:2023, the Essential Eight Maturity Model, NIST CSF 2.0, C2M2 Version 2.1, and the 2023 AESCSF Framework Core—and mandates compliance at maturity level 2 or equivalent. This approach gives responsible entities a clear, auditable benchmark for cyber security compliance.

No equivalent framework is prescribed or referenced for the personnel hazard domain. Section 9A requires responsible entities to assess the suitability of critical workers, conduct AusCheck background checks, and proactively monitor ongoing suitability—but does not specify *how* suitability assessments should be conducted, what standard of assessment is acceptable, or what framework underpins the suitability decision. The Rules mandate the *outcome* (a suitable workforce) without prescribing the *methodology*.

This creates a structural asymmetry: cyber security obligations are measurable and auditable against named frameworks at specified maturity levels, while personnel security obligations are open to interpretation and variable in quality. The predictable consequence is that many responsible entities—particularly those without in-house security expertise—will default to the minimum: an AusCheck check plus whatever ad hoc HR processes they already have in place. This will not discharge the obligations in sections 9A(2) and 9A(3) as intended.

The solution already exists. **AS 4811:2022 *Workforce Screening*** is the current Australian Standard for personnel screening and suitability assessment. It contains 19 mandatory ("must"/"shall") clauses and 73 recommended ("should") clauses, providing a comprehensive, structured, and auditable framework that directly addresses the obligations the Exposure Draft seeks to impose.

AS 4811:2022 is not untested in the national security context. It is already the named standard for DISP Entry Level membership, where the Defence Industry Security Office requires conformance with the Standard as a condition of participation. If AS 4811:2022 is considered fit for purpose to protect Defence industry personnel security, there is no policy rationale for excluding it from critical infrastructure—particularly when the Exposure Draft itself acknowledges that the threats to critical infrastructure from espionage, insider threat, and foreign interference are equivalent to those facing Defence.

Furthermore, the Department of Home Affairs' own Protective Security Policy Framework references AS 4811:2022 as the recommended standard for workforce screening. It is therefore incongruent for the Department to recommend the Standard in its own security framework while omitting it from the Enhanced CIRMP Rules that it administers. Placing AS 4811:2022 into the Rules would align the CIRMP with the PSPF and create a consistent national approach to personnel security across government and critical infrastructure.

3. The AusCheck Gap: Why Background Checking Alone Is Insufficient

We support the mandate for AusCheck background checking as a necessary foundation. However, the Exposure Draft itself describes threats that AusCheck was not designed to detect.

The Consultation Paper and the Exposure Draft's covering summary identify the core personnel threats to critical infrastructure as: espionage and foreign interference by state actors, exploitation of trusted insiders through coercion or inducement, sabotage through misuse of privileged access, and the compromise of credentials and privileged access to critical systems. These are the threats that section 9A(2) requires responsible entities to mitigate.

AusCheck verifies identity, checks criminal history (via the Australian Criminal Intelligence Commission), and includes an intelligence assessment. It is a *check*—it returns information. It does not, and was not designed to, make a *suitability determination for the employer*. This distinction is critical. The responsible entity still bears the obligation to decide whether a person is suitable to access critical systems—AusCheck provides inputs to that decision, but does not make it. Without a structured suitability assessment framework, the employer has no methodology for translating AusCheck results into a defensible suitability determination. It does not assess a person's character, integrity, honesty, or tolerance for risk. It does not identify coercive vulnerabilities, undisclosed financial distress, foreign influence exposure, or ideological motivations. These are precisely the indicators that distinguish a trusted insider from a compromised one.

Critically, the AusCheck scheme's historical reference to workforce screening standards was to **AS 4811:2006**—a standard published almost 20 years ago. The 2006 standard did not require ongoing suitability assessment, did not mandate a structured risk assessment (adjudication) process, and

did not address continuous monitoring of personnel risk. It was a product of a different threat environment.

AS 4811:2022 was published specifically to address these shortcomings. It introduces mandatory requirements that directly map to the obligations in section 9A:

Exposure Draft Obligation	AusCheck Alone	AS 4811:2022
s9A(3)(a): Assess suitability of critical workers with access to critical systems	Returns check results (identity, criminal history, intelligence). Does not make or guide the suitability decision.	Mandates a structured 1:1 suitability interview for high-risk roles. Requires formal risk assessment (adjudication) producing a documented Green/Amber/Red suitability determination.
s9A(3)(c): Proactively monitor ongoing suitability	Point-in-time check. Revalidation at 5-year intervals. No continuous monitoring mechanism.	Mandates full-lifecycle screening including ongoing suitability assessments (e.g. annual check-ins) and security protocols for separating personnel.
s9A(2)(b): Minimise risk of compromise and misuse of credentials	Does not assess behavioural indicators, coercive vulnerabilities, or foreign influence exposure.	Suitability interview framework specifically designed to identify character, integrity, honesty, and vulnerability to coercion—the core insider threat indicators.
s9A(3)(d): Minimise risks posed by incoming or outgoing critical workers	Pre-employment check only. No offboarding security protocol.	Addresses full employment lifecycle including separation protocols and risk management for departing personnel.

The table above demonstrates that AusCheck and AS 4811:2022 are complementary, not competing. AusCheck provides the intelligence-backed background check; AS 4811:2022 provides the suitability assessment framework that transforms check results into a defensible, auditable personnel risk decision. One without the other leaves the obligation partially discharged.

4. Offshore Critical Workers Accessing Australian Critical Infrastructure

Section 9A(5)(c) of the Exposure Draft acknowledges that offshore critical workers may not be able to undergo an AusCheck background check or hold an NV1 clearance. In those cases, the responsible entity must outline the associated risks in their CIRMP and take reasonably practicable actions to minimise or eliminate the material risk.

The Department's response in Attachment B is unequivocal: it does not consider any foreign check to be equivalent to the requirements placed on onshore workers, and requires "appropriate

mitigations" to accompany recruitment and continuous monitoring of offshore workers.

This creates a practical gap. Many offshore critical workers—particularly managed service provider staff, vendor engineers, and remote operations personnel—have direct access to Australian critical infrastructure systems, including operational technology, SCADA systems, and business-critical data. The FOCI material risk in section 6A(b) applies equally to these workers, yet the Rules offer no guidance on what "appropriate mitigations" look like.

Cleard Life's Critical Infrastructure Clearance product addresses this gap directly. It is a structured suitability assessment conducted to AS 4811:2022—distinct from both AGSVA national security clearances and AusCheck background checks—that can be applied to offshore workers regardless of their jurisdiction. The assessment includes a structured interview, risk assessment (adjudication), and a documented suitability determination. Critically, it does not depend on access to Australian government databases; it is an investigative and evaluative process that assesses the *person*—their character, integrity, honesty, and vulnerability to coercion—not just the records available about them. This gives responsible entities a documented, defensible basis for their CIRMP—precisely the "appropriate mitigation" the Department expects but has not defined.

5. Ongoing Suitability: Closing the Five-Year Gap

Section 9A(3)(c) introduces a significant new obligation: responsible entities must "proactively monitor, identify and take action in relation to any developments or changes that may affect the ongoing suitability of an offshore or onshore critical worker." This is continuous vetting language and represents a substantial uplift from the status quo.

However, section 9A(7)(c) sets the AusCheck revalidation cycle at a minimum of every 5 years. A 5-year gap between formal reassessments is fundamentally inconsistent with a "proactive monitoring" obligation, particularly in the threat environment described by the Director-General of Security and referenced throughout the Consultation Paper. Personnel circumstances change: financial distress, relationship breakdown, foreign travel, new foreign associations, health changes, and behavioural indicators can all emerge within months, not years.

AS 4811:2022 directly addresses this gap. Section 2.8.8.3 of the Standard prescribes 15 specific criteria for ongoing suitability assessment, covering:

- changes in personal circumstances (relationships, living arrangements, dependants)
- changes in financial circumstances (debt, bankruptcy, unexplained wealth)
- criminal charges, convictions, or adverse findings
- performance management, misconduct, or disciplinary actions
- workplace security violations or breaches of policy
- association with persons or groups of security concern
- unauthorised overseas travel or undisclosed foreign contacts
- contact with foreign nationals or foreign government representatives
- attitudes toward security protocols and willingness to comply

- misuse or attempted misuse of access privileges
- substance use (drugs and alcohol) that may affect suitability
- mental health changes that may affect capacity or vulnerability
- gambling behaviour that may create financial vulnerability
- digital and online behaviour that may indicate risk
- any other matter that may affect the person's ongoing suitability, loyalty, or reliability

These 15 criteria map directly to the insider threat indicators the Enhanced CIRMP Rules are designed to detect. None of them are assessed by a 5-yearly AusCheck revalidation. They require a structured, periodic reassessment process—conducted annually or at least at regular intervals—that is purpose-built for ongoing suitability.

Cleard Life operationalises this through our periodic check-in services, aligned to AS 4811:2022 section 2.8.8.3. Our check-in is a comprehensive confidential questionnaire covering all 15 criteria, evaluated against the worker's previous suitability assessment to identify changes in risk posture. The frequency is calibrated to the risk profile and position—it can be conducted annually, at longer intervals for lower-risk roles, or at shorter intervals where the threat environment or access level warrants it. For AGSVA clearance holders, we also provide Vetting Vantage Point—a 3-monthly check-in designed to satisfy DISO's Insider Risk Management Program requirements. This is a practical, commercially available mechanism that enables responsible entities to discharge the section 9A(3)(c) obligation without waiting five years between formal touchpoints.

The PSPF itself reinforces this position. Table 33 of the PSPF (*Procedures for Assessing and Managing Ongoing Suitability*) sets out ongoing suitability procedures for both uncleared and security-cleared personnel. Critically, the PSPF makes the following procedures **mandatory even for uncleared personnel**:

Procedure	Uncleared Personnel	Security Cleared Personnel
Building personnel security into performance management	**Mandatory**	Mandatory
Periodic employment suitability check	**Mandatory**	Mandatory
Annual security check	Recommended	Mandatory
Contact reporting obligations	Recommended	Mandatory
Security incident reporting and follow-up	Recommended	Mandatory
Collecting and assessing information on changes in personal circumstances	Recommended	Mandatory

The implication is clear: the Australian Government already considers periodic employment suitability checks mandatory for its own uncleared workforce. Critical infrastructure workers with privileged access to critical systems—systems whose compromise could prejudice the social or

economic stability, or national security of Australia—should be held to at least the same standard. A 5-year AusCheck revalidation cycle, with no structured periodic suitability assessment in between, falls below what the PSPF already requires for uncleared Commonwealth personnel.

For entities in the Defence Industry Security Program (DISP), annual or periodic check-ins for personnel are already accepted practice aligned with PSPF requirements. The Enhanced CIRMP Rules should adopt the same expectation for critical infrastructure, ensuring consistency across Australia's security frameworks.

6. Recommendations

We make four recommendations for the finalisation of the Enhanced CIRMP Rules and the development of accompanying guidance:

Recommendation 1: Reference AS 4811:2022 as the personnel security framework

The Enhanced CIRMP Rules or accompanying guidance should explicitly reference AS 4811:2022 *Workforce Screening* as the recognised Australian Standard for conducting suitability assessments under section 9A. This would mirror the approach taken for cyber security in section 8A(3), where specific frameworks are listed and maturity levels are prescribed.

Just as an entity can demonstrate cyber compliance by meeting maturity level 2 of the Essential Eight or NIST CSF 2.0, an entity should be able to demonstrate personnel security compliance by conducting suitability assessments conformant with AS 4811:2022. This provides a clear, auditable benchmark that the current drafting lacks.

Conformance with AS 4811:2022 should be accepted as satisfying the suitability assessment requirements in sections 9A(3)(a), 9A(3)(c), 9A(3)(d), and 9A(8), providing responsible entities with a defined pathway to compliance and enabling the Department to assess the quality of personnel security programs against a national standard—not against undefined and variable internal processes.

Recommendation 2: Require structured suitability interviews for critical workers with access to critical systems

The guidance accompanying the Rules should make clear that a suitability assessment under section 9A(3)(a) requires more than a transactional background check. For critical workers with access to critical systems (as defined in the Exposure Draft), the assessment must include a structured, one-on-one suitability interview as mandated by AS 4811:2022.

This is the only established, defensible method to assess the character, integrity, honesty, and vulnerability indicators that distinguish insider threat risk from routine employment risk. Processes that rely solely on automated checks or AusCheck results without a suitability interview will not address the material risks described in section 9A(2).

Recommendation 3: Define "appropriate mitigations" for offshore critical workers using AS 4811:2022

The guidance should specify that for offshore critical workers who cannot undergo AusCheck or hold an NV1 clearance (section 9A(5)(c)), a suitability assessment conducted in conformance with AS 4811:2022 by a certified-conformant provider constitutes an "appropriate mitigation" for the purposes of the CIRMP.

This gives responsible entities a practical, available pathway to discharge their obligation under section 9A(5)(c)(ii) and provides the Department with assurance that offshore personnel accessing Australian critical infrastructure have been assessed to a recognised national standard—rather than leaving the definition of "appropriate mitigations" to each entity's discretion.

It is important to note that a suitability assessment conducted to AS 4811:2022 is distinct from both an AGSVA national security clearance (e.g. NV1) and an AusCheck background check. It is a purpose-built workforce screening assessment that evaluates character, integrity, honesty, and vulnerability to coercion through structured interview and risk assessment. It does not require access to Australian government databases and can therefore be applied to offshore workers in any jurisdiction. For the highest-risk offshore roles with privileged OT or control system access, guidance should recognise a suitability assessment conformant with AS 4811:2022 as the expected standard.

Recommendation 4: Address the five-year revalidation gap with annual or periodic suitability check-ins aligned to AS 4811:2022 section 2.8.8.3

Section 9A(3)(c) requires proactive monitoring of ongoing suitability. The guidance should clarify that the 5-year AusCheck revalidation cycle (section 9A(7)(c)) is a *minimum* for formal background check renewal, and that responsible entities are expected to implement periodic suitability reassessments at shorter intervals to discharge their proactive monitoring obligation.

AS 4811:2022 section 2.8.8.3 prescribes 15 specific criteria for ongoing suitability assessment—covering changes in personal, financial, and professional circumstances, associations with persons of security concern, foreign contacts, misuse of access privileges, substance use, and other indicators. The Department's guidance should reference annual or at least periodic check-ins against these criteria—consistent with existing DISP and PSPF practice—as the expected mechanism for meeting the section 9A(3)(c) obligation.

Without this guidance, many responsible entities will treat the 5-year AusCheck revalidation as their sole ongoing suitability mechanism—leaving up to five years in which none of the 15 ongoing suitability criteria are formally assessed. This is incompatible with the proactive monitoring intent of section 9A(3)(c) and with the threat environment described throughout the Consultation Paper.

7. The Case for Structural Parity Between Cyber and Personnel Frameworks

The Consultation Paper and the Director-General's Annual Threat Assessment 2025 make clear that the threat to critical infrastructure is not solely cyber. Espionage, insider threat, and foreign interference are assessed as among the most significant national security threats to Australia. The AIC/ASIO *Cost of Espionage* report estimates insider threats involving state-sponsored actors could cost up to $324.8 million per incident.

Despite this, the Exposure Draft gives cyber security obligations a defined, measurable framework structure (five named standards, specified maturity levels, compliance pathways), while personnel security obligations are left without equivalent scaffolding. The following comparison illustrates the disparity:

Attribute	Cyber (s8A)	Personnel (s9A)
Named framework(s)	Yes — 5 listed	None
Specified maturity level	Yes — Level 2	None
Equivalent framework pathway	Yes — s8A(4)	None
Auditable compliance benchmark	Yes	No — suitability assessment undefined
Australian Standard available	AS ISO/IEC 27001:2023 (listed)	AS 4811:2022 (not listed)
Mandatory + recommended clauses	Varies by framework	19 mandatory, 73 recommended
Already adopted in Defence context	N/A	Yes — named standard for DISP Entry Level
Referenced in Home Affairs' own PSPF	N/A	Yes — recommended standard for workforce screening

Referencing AS 4811:2022 in the Rules or guidance would resolve this disparity. It would not mandate a single approach—responsible entities could still choose equivalent frameworks or internal programs, just as they can for cyber security under section 8A(4). But it would establish a benchmark that makes personnel security obligations measurable, auditable, and consistent across the critical infrastructure sector.

8. About Cleard Life

Cleard Life is an Australian-owned specialist provider of workforce screening, personnel suitability assessment, and security clearance management services. Our capabilities directly relevant to this

submission include:

AS 4811:2022 Conformance: First organisation in Australia to achieve auditor-certified conformance to all 19 mandatory and all 73 recommended clauses of AS 4811:2022 *Workforce Screening*.

AGSVA Clearance Portfolio Management: Former AGSVA panel member with over a decade of experience processing Baseline, NV1, and NV2 national security clearances. We currently manage a large AGSVA clearance portfolio for DISP members and aspiring DISP members across Defence, critical infrastructure, aerospace, and cyber security sectors.

Critical Infrastructure Clearance: Our purpose-built suitability assessment product for critical infrastructure, conducted to AS 4811:2022. This is distinct from AGSVA national security clearances and AusCheck background checks. It includes structured 1:1 suitability interviews and formal risk assessment (adjudication) producing documented Green/Amber/Red suitability determinations across multiple assessment levels (CL0–CL3).

Periodic Check-In (Ongoing Suitability): Structured periodic reassessments aligned to AS 4811:2022 section 2.8.8.3, covering all 15 ongoing suitability criteria. Frequency calibrated to risk and position—annual, longer, or shorter intervals. For AGSVA clearance holders, our Vetting Vantage Point product provides 3-monthly check-ins to satisfy DISO's Insider Risk Management Program. Available for DISP members and critical infrastructure entities.

Critical Infrastructure Experience: Active provider to critical infrastructure entities across energy, water, transport, and communications sectors.

Defence Trailblazer Partnership: Partnered with UNSW Canberra (ADFA) through the Defence Trailblazer program to develop AI-driven personnel security capability for national security and critical infrastructure agencies, as well as democratise personnel screening to enable employers a suitability screening platform where they can conduct adjudications themselves.

9. Conclusion

The Enhanced CIRMP Rules represent a necessary and welcome uplift to the security of Australia's most critical assets. The personnel hazard provisions in section 9A are well-directed and address genuine threats. However, without a recognised framework for suitability assessment, these provisions risk being implemented inconsistently and at a standard below what the threat environment demands.

AS 4811:2022 is the current Australian Standard for workforce screening. With 19 mandatory and 73 recommended clauses, it is comprehensive, commercially viable, immediately available, and directly addresses every personnel security obligation in the Exposure Draft. Referencing it in the Enhanced CIRMP Rules or accompanying guidance would give responsible entities the same clarity for personnel security that the five listed cyber frameworks provide for information security.

We welcome the opportunity to discuss these recommendations with the Department and to contribute to the development of best practice guidance for the personnel hazard provisions.

Contact
Edward Barker, Director
Cleard Life Vetting Agency
Ph: 02 6171 4171
Email: info@cleard.life
Web: www.cleard.life

[End of Submission]