To the Critical Infrastructure Security Centre
Department of Home Affairs

From Goldilock Secure
Date 4 February 2026

Subject: Formal endorsement of submission on proposed enhancements to the CIRMP Rules

Dear Sir or Madam,

On behalf of Goldilock Secure, I write to formally endorse our submission responding to the consultation on proposed amendments to the Critical Infrastructure Risk Management Program Rules.

Goldilock strongly supports the Department's objective to strengthen the resilience of Australia's critical infrastructure, particularly in environments where cyber compromise can result in material operational, safety, or national consequences. As the threat landscape continues to evolve, effective risk management must address not only prevention, but also credible, pre-authorised mechanisms for containment, consequence reduction, and assured recovery when preventative measures are bypassed.

Contemporary cyber incidents demonstrate that highly capable threat actors exploit complexity, persistence, and legitimate connectivity pathways to move laterally across environments and degrade software-based controls over time. In such conditions, resilience depends on the ability to retain deterministic control over connectivity between critical systems and domains, including through measures that remain effective under degraded cyber conditions.

The submission provided reflects Goldilock's view that physical-layer separation represents a legitimate and necessary class of mitigative control for high-consequence environments. When incorporated into risk management, incident response, and recovery planning, such controls materially limit blast radius, constrain systemic contagion, and support faster, more assured restoration of services. We believe this approach closely aligns with the intent of the proposed CIRMP enhancements, particularly regarding network segregation, cybersecurity maturity uplift, and recovery preparedness.

Goldilock's Australian operations are led by Mr Shane Read, an experienced Chief Information Security Officer and former Federal Government and Defence employee. Mr Read has spent his career designing, implementing, and operating security programs across government, defence, and critical infrastructure environments, with a focus on reducing systemic cyber risk and improving resilience outcomes. While I remain available for engagement as required, Mr Read is fully empowered by Goldilock to represent the company in Australia and to support the delivery of our mission.

That mission is to assist Australia and other democratically aligned nations to maintain sovereign control over their critical infrastructure by enabling deterministic, reliable control of network connectivity at points where compromise would otherwise result in unacceptable national or societal impact. We view this capability as foundational to national resilience in an increasingly contested cyber environment.

Goldilock appreciates the opportunity to contribute to this important consultation process and would welcome further engagement with the Department as the CIRMP framework continues to evolve. We remain committed to supporting outcomes that are practical, proportionate, and aligned with Australia's sovereign security and resilience objectives.

Yours sincerely,

[redacted]

Tony Hasek
Chief Executive Officer
Goldilock Secure

Date 4 February 2026

SUBMISSION BY GOLDILOCK SECURE ON PROPOSED AMENDMENTS TO THE CIRMP RULES

To: Critical Infrastructure Security Centre
Department of Home Affairs

From: Goldilock Secure

EXECUTIVE SUMMARY

Goldilock welcomes the opportunity to comment on the proposed amendments to the Critical Infrastructure Risk Management Program Rules. We support the Department's intent to strengthen resilience across critical infrastructure assets by improving expectations around network segregation, cybersecurity maturity, incident response, and recovery preparedness.

As cyber threats increasingly demonstrate persistence and high-impact outcomes, effective risk management must place greater emphasis on mitigating consequences when preventative measures are bypassed. In this context, we submit that physical-layer separation and physical connection control should be recognised as a legitimate and effective class of mitigative control within the CIRMP framework, particularly where the consequences of compromise are significant.

SHIFTING THE DEFENSIVE FOCUS TOWARD CONSEQUENCE MANAGEMENT

The consultation paper appropriately recognises that risk management must address both the likelihood of cyber hazards and the impact that occurs once those hazards materialise.

Recent incidents across critical infrastructure sectors show that attackers often remain undetected for extended periods, exploit legitimate connectivity pathways, and degrade software-based controls over time. In many cases, response actions are delayed due to uncertainty, operational risk, or governance constraints.

This highlights the limitations of relying solely on software-based preventative controls and reinforces the need for measures that remain effective under degraded cyber conditions.

PHYSICAL-LAYER SEPARATION AS A MITIGATIVE CONTROL

For clarity, this submission uses the term Physical Connection Control (PCC) to describe deterministic, hardware-enforced separation at the physical layer that governs whether connectivity between systems or domains exists.

Physical-layer separation operates at the level of the physical connection itself, determining whether connectivity exists between systems or domains. Unlike software-defined segmentation, physical connection control enforces deterministic separation that is independent of operating systems, credentials, or policy enforcement mechanisms.

When incorporated into a broader risk management approach, physical separation can materially limit lateral movement, reduce contagion between domains, and constrain the blast radius of a cyber incident. This makes it particularly suitable for environments where operational, safety, or national consequences are high.

ALIGNMENT WITH PROPOSED CIRMP ENHANCEMENTS

The proposed requirement for high-risk assets to achieve higher levels of cybersecurity maturity by 2028 is appropriate. Physical separation supports this objective by reducing the attack surface, enabling controlled connectivity models, and providing assurance that segmentation remains enforceable during incidents.

The consultation paper also calls for the greatest practical level of network segregation. In complex IT and OT environments, uncontrolled connectivity between business systems, suppliers, and operational networks remains a

primary pathway for systemic compromise. Physical separation enables a compartmentalisation-of-risk approach, allowing domains to remain isolated by default and connected only under defined conditions.

From an incident response and recovery perspective, pre-planned separation mechanisms provide a credible back-stop. They allow operators to rapidly isolate affected systems, protect recovery environments from contamination, and reconnect only after integrity checks and explicit authorisation. This improves response confidence and supports faster, more assured recovery.

SOVEREIGN BUILD AND TRUSTED SUPPLY CHAIN CONSIDERATIONS

An additional factor relevant to the effective management of critical infrastructure risk is assurance of the integrity and provenance of the security controls themselves.

In the current threat environment, where state-linked cyber actors are known to exploit long-term persistence, supply chain dependencies, and unmanaged connectivity, confidence in both control effectiveness and component provenance is critical. This is particularly relevant where controls are expected to operate as mitigative mechanisms during periods of elevated threat or degraded cyber conditions.

For high-consequence environments, risk treatment decisions increasingly consider the manufacturing jurisdiction and component supply chains of technologies used to enforce segmentation, isolation, and recovery controls. This aligns with broader government expectations regarding trusted vendors, sovereign resilience, and the avoidance of hidden dependencies in critical infrastructure.

Goldilock's physical connection control technology is available in two sovereign manufacturing variants. One variant is manufactured in the United States using components sourced exclusively from within the United States. The second variant is manufactured in the United Kingdom using components sourced solely from NATO-aligned nations. Neither variant incorporates components originating from jurisdictions assessed as high risk to Australian national security interests.

From a CIRMP perspective, this approach supports risk management outcomes by reducing the likelihood that controls relied upon for containment and recovery introduce additional, unmanaged supply chain risk.

IMPLEMENTATION CONSIDERATIONS

We are not advocating prescriptive technical mandates. Rather, supporting guidance could encourage entities to consider identifying physical isolation points for critical dependencies, defining conditions and authority for activating separation, integrating separation into incident response and recovery plans, and testing isolation and reconnection as part of resilience exercises.

These considerations align with the consultation paper's emphasis on preparedness, proportionality, and accountable decision-making.

SUPPORTING SOCI ALIGNMENT AND TECHNICAL ASSURANCE

To support the considerations outlined in this submission, Goldilock has provided two accompanying annexes.

Annex A, titled *SOCI Alignment Statement – Physical Separation, Sovereign Supply Chain, and Critical Infrastructure Resilience*, explains how physical-layer separation and trusted manufacturing provenance align with obligations under the Security of Critical Infrastructure Act and complement the proposed CIRMP enhancements. This annex includes concise SOCI and CIRMP alignment tables to assist review.

Annex B, titled *Technical and Sovereign Assurance Details*, provides supporting information on supply chain integrity, sovereign manufacturing provenance, and the technical characteristics relevant to segmentation, containment, and recovery in high-consequence environments.

SUGGESTED GUIDANCE WORDING

Where cyber compromise may result in significant operational, safety, or national impacts, entities should consider mitigative controls that remain effective under degraded cyber conditions, including physical separation or control mechanisms for physical connections, to support containment, resilience, and recovery.

CONCLUSION

Goldilock supports the Department's objective of strengthening critical infrastructure resilience through enhanced CIRMP requirements. As cyber threats evolve toward more destructive outcomes, effective risk management must include credible mitigative controls that limit consequences when preventative measures fail.

Physical-layer separation provides a technology-agnostic means of achieving this outcome and complements existing cybersecurity measures. Goldilock welcomes the opportunity to participate in further consultation or co-design activities to ensure the enhanced CIRMP framework is practical, proportionate, and effective for complex critical infrastructure environments

ANNEX A - SOCI ALIGNMENT STATEMENT

Physical Separation, Sovereign Supply Chain, and Critical Infrastructure Resilience

Goldilock's approach to physical connection control and sovereign manufacturing aligns with the intent and obligations of the Security of Critical Infrastructure Act, particularly regarding risk management, resilience, and recovery for high-consequence assets.

Under the SOCI framework, responsible entities are required to establish and maintain a Critical Infrastructure Risk Management Program that identifies hazards, assesses material risks, and implements proportionate controls to reduce the likelihood and impact of adverse events. Cyber compromise, lateral movement across interconnected systems, and reliance on opaque or high-risk supply chains represent material hazards in many critical infrastructure environments.

Physical-layer separation addresses these hazards by enabling deterministic control over connectivity between critical systems and domains. Unlike software-enforced controls, physical separation does not depend on operating systems, identity systems, or network policy engines and therefore remains effective under degraded cyber conditions. When used as part of a risk management program, such controls reduce blast radius, limit systemic contagion, and support faster containment and recovery.

Supply chain integrity is also a relevant consideration under SOCI, particularly where controls are relied upon to function during periods of heightened threat. Goldilock provides physical connection control technology in two sovereign manufacturing variants: one manufactured in the United States using exclusively US-sourced components, and one manufactured in the United Kingdom using components sourced solely from NATO-aligned nations. Neither variant incorporates components from jurisdictions assessed as high risk to Australian national security interests. This approach supports SOCI objectives by reducing hidden dependencies and improving confidence in the reliability of mitigative controls.

Physical separation and trusted supply chain assurance support SOCI outcomes by strengthening resilience, enabling proportionate risk treatment, and ensuring that response and recovery actions remain viable even when preventative cyber measures are bypassed. These controls complement rather than replace existing cybersecurity measures and are intended to be applied selectively where the consequences warrant higher assurance.

SOCI Act concept	SOCI intent	Relevant technical and sovereign assurance elements	Alignment to SOCI obligations
Critical Infrastructure Risk Management Program	Require responsible entities to establish, maintain, and comply with a written risk management program	Formal treatment of physical separation and supply chain integrity as part of risk management	Demonstrates structured identification and treatment of risks beyond preventative cyber controls
Hazard identification	Identify hazards that could have a relevant impact on critical infrastructure	Recognition of cyber compromise, lateral movement, and supply chain dependency as hazards	Treats uncontrolled connectivity and untrusted supply chains as material hazards
Material risk	Identify risks that could have a significant operational, safety, or national security impact	Physical-layer separation applied to high-consequence domains	Focuses mitigative controls where consequences are highest, consistent with SOCI proportionality
Information security hazards	Address risks arising from unauthorised access, compromise, or misuse of systems	Deterministic physical connection control independent of software enforcement	Provides assurance where software-based controls may be degraded or bypassed
Systems of national significance	Strengthen resilience for assets with elevated consequence profiles	Physical separation as a last-line mitigative control	Supports higher assurance expectations for nationally significant systems
Resilience	Ensure assets can withstand, adapt to, and recover from adverse events	Compartmentalisation of risk and blast-radius limitation	Improves system survivability during prolonged or sophisticated cyber events
Prevention and mitigation	Reduce likelihood and impact of hazards	Physical separation as a mitigative control when prevention fails	Complements preventative controls by reducing consequence
Incident response	Enable timely and effective response to incidents	Pre-planned physical isolation points and authority	Allows rapid containment without reliance on compromised systems
Recovery	Support restoration of systems following incidents	Isolation of backup and recovery environments	Protects recovery processes from reinfection or contamination
Supply chain hazards	Identify and manage risks arising from third-party dependencies	Sovereign manufacturing and trusted component sourcing	Reduces risk introduced by opaque or high-risk supply chains
Trusted vendors	Ensure confidence in providers supporting critical functions	US-manufactured (US-only components) and UK-manufactured (NATO-only components) variants	Aligns control selection with trusted supplier expectations under SOCI
Avoidance of high-risk dependencies	Reduce exposure to foreign interference or coercion risks	Explicit exclusion of components from high-risk jurisdictions	Supports national security risk reduction objectives
Governance and accountability	Ensure clear authority and decision-making	Defined conditions for activation of separation	Enables auditable, pre-authorised actions during incidents
Proportionality	Apply controls appropriate to risk and consequence	Optional, risk-based deployment of physical separation	Avoids prescriptive mandates while supporting SOCI intent
Ongoing risk review	Maintain effectiveness of risk controls over time	Hardware-enforced controls that do not degrade with software complexity	Supports sustained compliance and resilience over the asset lifecycle

RELATIONSHIP TO CIRMP ENHANCEMENTS

The proposed enhancements to the Critical Infrastructure Risk Management Program Rules build upon the SOCI Act by providing greater clarity around cybersecurity maturity, network segregation, response preparedness, and recovery assurance. Physical-layer separation and sovereign supply chain assurance align directly with these enhancements by supporting mitigative controls that reduce impact when cyber hazards materialise.

Table A2 – Alignment to Proposed CIRMP Enhancements

CIRMP focus area	Supporting outcome
Network segregation	Absolute separation between critical domains
Cybersecurity maturity uplift	Controls remain effective under degraded cyber conditions
Mitigative controls	Consequence reduction when prevention fails
Contagion control	Compartmentalisation of risk across IT and OT
Response preparedness	Rapid, deterministic isolation
Recovery assurance	Controlled reconnection after integrity validation
Governance	Auditable, pre-authorised connectivity decisions

Within a CIRMP context, physical separation provides a practical mechanism for achieving the highest level of network segregation and enabling the compartmentalisation of risk across complex IT and OT environments. Trusted manufacturing provenance further supports CIRMP objectives by ensuring that controls relied upon for containment and recovery do not themselves introduce unmanaged risk.

Taken together, these measures support a coherent SOCI-aligned approach to critical infrastructure risk management, in which prevention, mitigation, response, and recovery are treated as integrated elements of resilience rather than isolated controls.

ANNEX B - TECHNICAL AND SOVEREIGN ASSURANCE DETAILS

Purpose

This annex provides supporting technical and sovereign assurance information relevant to the consultation on proposed enhancements to the Critical Infrastructure Risk Management Program Rules. It addresses supply chain integrity, manufacturing provenance, and the reliability of controls used to enforce segmentation, containment, and recovery in high-consequence environments.

Technical characteristics relevant to CIRMP outcomes

Physical connection control operates at the level of the physical link itself, determining whether connectivity between systems or domains exists. This characteristic provides several properties relevant to CIRMP risk management objectives.

Physical separation is deterministic, enforcing a clear, connected-or-disconnected state that is independent of operating systems, identity systems, software policies, or network management platforms. As a result, it remains effective even when parts of an environment are compromised or operating under degraded conditions.

When used to control connectivity between critical domains, such mechanisms materially limit lateral movement, reduce the potential for contagion across environments, and constrain the blast radius of a cyber incident. This supports faster containment and more assured recovery.

Relevance to segmentation, containment, and recovery planning

When physical separation mechanisms are incorporated into network architecture and operational planning, they can support a range of CIRMP-aligned outcomes, including enforcement of deliberate, auditable segmentation, pre-planned isolation points for incident response, protection of backup and recovery environments from contamination, and controlled reconnection following integrity verification and authorisation.

These characteristics complement existing preventative cybersecurity measures and provide additional assurance where consequences of compromise are significant.

Supply chain integrity and risk management

Assurance of supply chain integrity is a material consideration in the effective management of critical infrastructure risk. Where security controls are relied upon to function during periods of elevated threat or degraded cyber conditions, the provenance and component sourcing of those controls directly affect confidence in their reliability and suitability.

In the current threat environment, where state-linked cyber actors are known to exploit long-term persistence, supply chain dependencies, and unmanaged connectivity, assurance of both control effectiveness and component provenance is critical. Controls that introduce hidden or opaque dependencies can themselves become sources of unmanaged risk.

From a CIRMP perspective, supply chain integrity supports resilience objectives by reducing the likelihood that mitigative controls fail, degrade, or behave unpredictably when they are most needed.

Sovereign manufacturing and component provenance

Goldilock's physical connection control technology is available in two sovereign manufacturing variants.

One variant is manufactured in the United States using components sourced exclusively from within the United States. The second variant is manufactured in the United Kingdom using components sourced solely from NATO-aligned nations.

Neither manufacturing variant incorporates components originating from jurisdictions assessed as high risk to Australian national security interests.

This approach is intended to provide transparency, assurance, and confidence in the supply chains supporting controls that may be relied upon as last line mitigative mechanisms for segmentation, containment, and recovery.

Assurance Summary

From a CIRMP perspective, trusted supply chains and sovereign manufacturing provenance are relevant considerations when selecting controls that underpin critical segmentation, containment, and recovery functions. Physical connection control mechanisms that are transparently manufactured within trusted jurisdictions and operate independently of software enforcement provide additional confidence in the resilience of critical infrastructure environments.