REQUEST FOR COMMENT RESPONSE

Proposed amendments to the Critical Infrastructure Risk Management Program Rules for high-risk asset classes

13 February 2026

I. INTRODUCTION

CrowdStrike appreciates the opportunity to provide our comments to the Department of Home Affairs on the proposed amendments to the Critical Infrastructure Risk Management Program Rules (CIRMP rules) for high-risk asset classes. We support the Australian Government's objective to strengthen the resilience of critical infrastructure (CI) in the face of increasing cyber threats, complex supply chains, and heightened foreign ownership, control or influence (FOCI) risks.

CrowdStrike is an international cybersecurity company, based in the United States, that protects businesses around the world from globally-distributed cyber threats. We have extensive experience helping organisations prevent data breaches with a range of cybersecurity products and services including cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace.

II. COMMENTS

A. Cyber Security Framework Uplift

The Department proposes to require entities to meet maturity level 2 of their chosen cyber maturity framework, an increase from the current level 1 requirement. CrowdStrike supports this uplift as a necessary response to the increasingly sophisticated threat landscape, particularly from state-sponsored threat actors like Vanguard Panda (Volt Typhoon), Operator Panda (Salt Typhoon), and Cozy Bear (APT29) that actively target CI.

We particularly support the emphasis on operational security outcomes, such as the ability to detect incidents, respond effectively, and recover services, rather than an exclusive focus on preventative controls.

While we support the maturity framework uplift, we recommend that the Department focus on the security outcomes achieved rather than strict compliance with specific framework levels. The consultation references maturity benchmarks (for example, C2M2 Maturity Indicator Level 2 or AESCSF Security Profile Level 2). These frameworks are useful reference points. However, the Rules and supporting guidance should clearly state that:

- Maturity models are benchmarks for expected capability, not certification schemes;
- Entities may select an appropriate framework and demonstrate equivalent maturity; and
- There is no requirement to obtain a formal certificate against a specific model.

Without this clarity, there is a risk that the market will treat maturity benchmarks as mandatory certifications, encouraging checkbox behaviour and diverting effort away from genuine operational uplift.

The proposed 18-month implementation period is reasonable as it will allow entities sufficient time to develop and execute uplift plans. We support the Department's stated intention to publish guidance clarifying what 'level 2' maturity looks like across different frameworks and encourage this guidance to focus on outcomes, evidence and risk management principles, rather than being an exhaustive control mapping.

B. Evidence quality

The effectiveness of CIRMP will depend heavily on what constitutes acceptable evidence for meeting the criteria. CIRMP artefacts should be capable of standing up to post-incident regulatory scrutiny, not merely forward-looking assurance checks. Flexible evidence pathways improve assurance outcomes by allowing entities to demonstrate maturity using artefacts that reflect real operational practices, rather than forcing uniform documentation that may obscure actual risk management.

We recommend the Department provide guidance to covered entities to clearly articulate what 'good evidence' looks like, including worked examples, and allow multiple evidence pathways, including internal assessments, independent reviews, and relevant assurance artefacts.

C. Critical Systems Network Protection

CrowdStrike strongly supports the proposal requiring entities to implement network segregation for critical systems. Network segregation is a fundamental security control that can significantly limit lateral movement during compromises and prevent attackers from reaching an organisation's most critical assets.

Recent threat intelligence confirms that sophisticated threat actors like Vanguard Panda specifically target externally facing networks to establish persistence and then laterally move to operational technology environments. The proposed requirements for inventory management, network segregation, logical access controls, and monitoring align with best practices for securing CI environments.

We recommend that the Department consider providing additional guidance on architectural

approaches for achieving effective network segregation, particularly in environments with legacy operational technology that may present integration challenges. Additionally, we suggest that the Department highlight that network segmentation should be implemented as part of a broader Zero Trust security strategy, which remains one of the most effective approaches for increasing cybersecurity.

D. Multi-Factor Authentication (MFA)

CrowdStrike strongly supports the requirement to implement phishing-resistant multi-factor authentication for critical systems access. Compromised credentials remain one of the primary vectors for initial access in significant breaches. The CIRMP recognises that there are fundamental problems with today's widely-used authentication architectures and increased risks from internet-facing networks, deployment of remote access capabilities, and compromised privileged user credentials. All organisations must respond by incorporating new authentication security protections into their cybersecurity security plan.

We recommend that the Department provide additional guidance on the capabilities to look for in a phishing-resistant MFA solution, and its effective deployment to ensure consistent implementation across different environments and technology stacks. For example, phishing-resistant MFA requires real-time security telemetry that includes data on endpoint behavior, cloud activity, and SaaS usage patterns to make contextual access decisions.

We also support the requirement for centralised logging of authentication attempts, as robust logging data underpins numerous core enterprise security functions and is essential for effective threat hunting and incident response.

Finally, Zero Trust security and identity threat protection approaches are important adjuncts to MFA-based guidance. They radically reduce or prevent lateral movement and privilege escalation during a compromise, and can stop attacks even if legitimate credentials are compromised and MFA is bypassed. We recommend that the Department supplement advice on MFA by emphasising the importance of Zero Trust more broadly in CI entities, even more secure identity strategies such as 'just-in-time' privilege issuance, and identity threat protection in preventing breaches.

E. Supply Chain Security Measures

The proposed supply chain measures, including vulnerability mapping and vendor assessment, address a critical security gap in many CI environments. Supply chain risks have become increasingly prominent in recent years, as demonstrated by the examples cited in the consultation paper regarding undeclared communications equipment in foreign state-made solar inverters.

Supply chain security is a complex third-party partner and vendor risk management problem that spans numerous disciplines. The proposed requirement to map supply chains for major

suppliers and critical systems is an essential first step in understanding and mitigating these risks.

We recommend that the Department develop specific guidance on how to assess Foreign Ownership, Control or Influence (FOCI) risks in vendors, including criteria that covered entities should consider when assessing 'foreign risk' in a vendor. While the FOCI Risk Assessment Guidance is referenced, more operational guidance would be beneficial for entities without extensive security resources.

We also recommend the Department encourage CI entities maintain a resilient and trusted supply chain by conducting real-time visibility and continuous monitoring of digital components and software dependencies, and the use of threat intelligence to identify supply chain vulnerabilities or compromises early.

F. Personnel Security Measures

CrowdStrike supports the proposal to strengthen personnel security requirements for trusted roles associated with CI. In our experience a holistic approach to personnel security that encompasses not only background checks but also ongoing monitoring, identity protection best practices, and security awareness training.

We are concerned that reliance on a single clearance pathway can introduce systemic workforce risk in time-critical operational environments. Clearance bottlenecks can arise from multiple factors outside the control of entities, including processing backlogs, surge demand following threat-driven policy changes, revalidation delays, assessor capacity constraints, and limited recognition of equivalent checks across jurisdictions. These bottlenecks can directly affect incident response capacity, continuity of 24/7 security operations, safe workforce rotation, and access to scarce specialist skills during cyber or operational emergencies.

We therefore recommend the Rules and guidance explicitly support multiple, risk-appropriate pathways to demonstrate personnel security, including recognition of equivalent vetting regimes, layered approaches combining background checks with role-based access controls and monitoring, and interim or conditional access arrangements.

G. Offshore access and cross-border data flows

We strongly recommend explicitly framing offshore access and cross-border data flows as risks to be managed, rather than proxies for insecurity to avoid unnecessary confusion. As the Department appreciates, modern security operations, including monitoring, incident response, and specialist support, often rely on distributed teams. Geography alone is not a reliable indicator of risk. Where restrictions are intended, they should be clearly articulated and justified in risk terms.

Where business-critical data is hosted or processed offshore, instead of using location as a proxy for risk, regardless of data location covered entities should focus on mitigations and assurances such as:

- Strong identity protection and just-in-time privilege access management;
- Clearly defined time-bound data retention and deletion processes;
- Comprehensive telemetry collection and real-time monitoring;
- Clear accountability for the protection of the data; and
- Full visibility of the controls applied to protect the entity's data at all stages.

H. Modern approaches to cybersecurity

Considering the importance to Australia of CI entities and the capability and determination of cyber adversaries, the Department should consider promoting additional adaptable, outcome-oriented modern cybersecurity practices that strengthen resilience without imposing disproportionate burdens on operators such as:

- Maintaining robust logging and comprehensive telemetry collection for effective detection and investigation throughout the IT environment;
- Conducting continuous threat hunting to identify intrusions early;
- Ensuring speed and precision in incident response to contain potential disruptions; and
- Using Managed Security Service Providers (MSSPs) to supplement internal security capacity.

This includes encouraging CI entities to adopt state-of-the-art technologies such as:

- Dedicated cloud security solutions to protect distributed data;
- Endpoint Detection and Response (EDR) technology coupled with a next-generation SIEM to provide real-time visibility and automated response capabilities across IT and OT environments; and
- Machine learning–based prevention, just-in-time (JIT) privileges, and Identity Threat Detection and Response (ITDR) to anticipate and block evolving adversary tactics.

III. SUMMARY OF RECOMMENDATIONS

Based on our analysis of the proposed amendments, CrowdStrike offers the following recommendations:

1. **Principles and outcomes over prescriptions:** While establishing minimum standards is important, we recommend that the final rules maintain flexibility for entities to implement frameworks appropriate to their specific risk profiles and technology environments. The rules should clearly position the proposed maturity models as reference benchmarks rather than exclusive requirements. They should focus on outcomes and risk management principles rather than being an exhaustive control

mapping. They should also explicitly support multiple evidence pathways to include mechanisms such as internal assessments and independent reviews to avoid applying one-size-fits-all requirements that do not reflect the diverse operating models among CI entities.

2. **Guidance on architectural approaches and Zero Trust:** We recommend the Department provides additional guidance for CI entities on architectural approaches for achieving effective network segregation in IT and OT environments; the importance of identity threat protection using modern approaches like issuing just-in-time privileges; and their role as part of an effective broader Zero Trust security strategy.

3. **Secure authentication:** We recommend the Department provide additional guidance on the capabilities to look for in a "phishing-resistant" MFA solution and its effective deployment; the importance of centralised logging of all authentication attempts.

4. **FOCI risk assessments:** To assist entities without extensive security resources we recommend the Department provides additional guidance to CI entities on how to effectively apply a risk management approach to assess foreign ownership, control or influence (FOCI) risks in vendors.

5. **Additional supply chain security measures:** We recommend the Department also encourages CI entities to maintain a resilient and trusted supply chain by conducting real-time visibility and continuous monitoring of digital components and software dependencies, and use threat intelligence to identify supply chain vulnerabilities or compromises early.

6. **Securing the workforce:** We recommend that the Rules and guidance explicitly support multiple, risk-appropriate pathways to demonstrate appropriate personnel security practices, such as recognising equivalent alternative vetting regimes and using layered access controls, to prevent systemic workforce risk from clearance bottlenecks.

7. **Explicitly support cross border data flows:** We recommend that the Department explicitly characterise offshore access and cross-border data flows as risks to be managed through controls and governance, to avoid geography being used as the primary proxy for trust and security.

8. **Encourage modern approaches to cybersecurity:** We recommend the Department encourage CI entities to adopt adaptable, outcome-oriented modern cybersecurity practices that strengthen resilience without imposing disproportionate burdens on operators, and state-of-the-art technologies. These should include conducting continuous hypothesis-driven threat hunting, and ensuring comprehensive telemetry collection throughout the IT and OT environments to provide real-time visibility and enable automated responses to potential disruptions.

IV. CONCLUSION

CrowdStrike supports the Department of Home Affairs' efforts to strengthen Australia's critical infrastructure security through enhanced CIRMP Rules. The proposed amendments represent a significant step toward addressing evolving threats, particularly from sophisticated state-sponsored actors targeting essential services.

As these amendments move forward, we recommend continued engagement with stakeholders to ensure the requirements are practically implementable across different sectors and technology environments. As underlying technologies and threat landscape evolve faster than law and policy, we also recommend that the final framework focus on principles rather than prescriptive requirements and include a clear mechanism for periodic revisions to ensure they remain aligned with emerging threats, new technologies and best practices.

We welcome the opportunity to discuss these matters with you in more detail. Additional public policy inquiries can be made to:

Drew Bagley

VP & Counsel, Privacy and Cyber Policy

Email: policy@crowdstrike.com

Brian Fletcher

Director, Public Policy APJ

V. ABOUT CROWDSTRIKE

CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft, and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity, and immediate time-to-value.

Learn more: https://www.crowdstrike.com/.