REQUEST FOR COMMENT RESPONSE

CrowdStrike Response to the Australian Department of Home Affairs Consultation Paper: Proposed Amendments to Enhance the Critical Infrastructure Risk Management Program Rules (CIRMP Rules)

1 May 2026

I. INTRODUCTION

CrowdStrike welcomes the opportunity to provide input on the Department of Home Affairs' proposed amendments to the Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006) 2023 (CIRMP Rules). We commend the Australian Government for its continued commitment to strengthening the resilience of critical infrastructure (CI) in an increasingly contested threat environment, and for its consultative approach to developing these reforms.

CrowdStrike is an international cybersecurity company based in the United States that protects businesses around the world from globally-distributed cyber threats. We have a significant presence in Australia and across the Asia-Pacific region, serving customers across CI sectors including energy, financial services, telecommunications, healthcare, and government. Our threat intelligence teams track more than 250 named adversaries globally, including the state-sponsored actors VANGUARD PANDA (VOLT TYPHOON), AQUATIC PANDA (SALT TYPHOON), and others that are specifically identified in this Consultation Paper as posing material risks to Australia's CI.

This operational experience gives CrowdStrike a unique vantage point from which to contribute to the development of the enhanced CIRMP Rules.

II. COMMENTS

CrowdStrike strongly supports the proposed enhancements to the CIRMP Rules. The proposed amendments to the CIRMP Rules for CI in Australia introduce a new tier of enhanced risk management obligations for high-risk CI sectors, shifting the regime from broad principles to more explicit, intelligence-informed security expectations. The proposed changes are supported by phased implementation timelines and potential new reporting obligations.

Outcome-Based Regulation and Technology Neutrality

CrowdStrike strongly supports the framework's principles-based, outcomes-focused approach to CI security regulation. We commend the framework's approach of specifying security outcomes such as achieving cybersecurity “Maturity Level 2”, implementing

phishing-resistant MFA, and maintaining supply chain vulnerability maps while allowing responsible entities flexibility in how they achieve those outcomes.

The Role of Advanced Security Technology

CrowdStrike recommends that the Department explicitly recognise the role of advanced security approaches as a key enabler of the enhanced requirements. The proposed CIRMP enhancements will require responsible entities to significantly uplift their security capabilities. Many of the capabilities required to achieve and sustain Maturity Level 2 compliance such as continuous monitoring, rapid incident detection and response, and comprehensive logging, are most effectively delivered through modern security platforms that leverage AI and machine learning to process and analyse security telemetry at scale. The guidance accompanying the enhanced CIRMP Rules should encourage entities to consider advanced security technology platforms and approaches to accelerate their security journey.

Regulatory Coherence and Avoiding Duplication

CrowdStrike supports the Department's commitment to reducing regulatory duplication. As the enhanced CIRMP Rules are developed, CrowdStrike recommends the requirements are mapped against other applicable regulatory frameworks including APRA's CPS 230, the Telecommunications Security and Risk Management Program Rules, and other sector-specific requirements to continue to identify and eliminate unnecessary duplication.

Preserve secure global cyber operations and managed services

CrowdStrike recommends that the final rules do not unintentionally discourage the very services that help operators identify and respond to advanced threats at speed. Many Australian operators depend on “follow-the-sun” cyber operations to detect and contain threats quickly. The rules should expressly permit those models where access is least-privilege, time-bound, customer-approved, strongly authenticated, logged, and subject to encryption, segregation, and documented personnel assurance.

III. All-Hazard Measures

All-Hazard 1: Consideration of Specified Risk Advice

The amendments proposed in this section aim to elevate the CIRMP to require CI entities to consider national-consequence risks that could impact social stability, economic stability, national security or defence. It orders CI entities to consider government-issued threat advice and systemic risks and formally integrate into their risk management programs as opposed to only considering asset-level risks.

Recommendations

Establish a dynamic mechanism for the Department to specify risk advice to CI entities that

clearly indicates what risks responsible entities must consider as part of their CIRMP**.** The dynamic nature of the threat landscape means that static, point-in-time regulatory requirements will always lag behind adversary tradecraft. A mechanism that allows the government to direct industry attention toward specific, intelligence-identified risks within the large amount of other information they receive from the Government, without mandating a particular response would be a pragmatic and proportionate approach, and reduce ambiguity for entities.

Provide structured guidance templates to assist responsible entities in documenting their consideration of specified risk advice within their CIRMP in the risk plans. Standardised documentation will reduce compliance burden and improve the quality of evidence available for audit purposes.

IV. Cyber and Information Security Hazard Measures

Cyber 1: Cyber Security Framework and Maturity Uplift

Under the proposed amendments, Entities must align with a recognised cybersecurity framework (e.g. Essential Eight ML2, NIST, ISO) or an equivalent, establishing a minimum maturity baseline at the 'Maturity Level 2'. This provides a measurable capability uplift for CI entities and critical sectors rather than purely principles-based compliance.

CrowdStrike strongly supports the inclusion of the NIST Cybersecurity Framework (CSF) 2.0 as a recognised framework. The CSF is a widely recognised and applied framework and its broad adoption across global CI sectors will facilitate benchmarking and information sharing.

Recommendations

Provide clear mapping guidance between the recognised frameworks at Maturity Level 2 for CI entities. This mapping will help CI entities understand the equivalencies and differences between the various frameworks, and subsequently make informed choices about which framework best suits their operational context.

Explicitly address operational technology (OT) environments in the framework guidance. A large number of CI entities operate complex OT environments that present distinct cybersecurity challenges not fully addressed by IT-focused frameworks. As noted in the Consultation Paper, OT components must be 'taken into account and appropriately protected.' This is good, however additional guidance on OT-specific controls and framework application would be valuable.

Actively encourage CI entities to consider AI-powered security capabilities as part of their Maturity Level 2 compliance pathway. Modern AI-native security platforms can significantly accelerate the achievement and maintenance of higher maturity levels by automating threat detection, response, and compliance monitoring functions that would otherwise require

substantial manual effort.

Cyber 2: Critical Systems Network Protection

The proposed amendments introduce a requirement for entities to identify and inventory critical systems, implement network segmentation, and ensure the ability to recover and rebuild systems, including maintaining operational continuity during compromise. This introduces explicit expectations around resilience, isolation, and recovery in cyber incidents.

CrowdStrike supports the proposed requirement for responsible entities to implement practical segregation between critical systems and other networks. Network segmentation and the isolation of critical systems from internet-facing and business specific environments is one of the most effective architectural controls available to CI entities, and are broadly aligned with established best practices and CrowdStrike's own recommendations to CI clients.

Recommendations

Emphasise the importance of continuous monitoring and detection capabilities alongside network segmentation. Segmentation reduces the attack surface and slows lateral movement, but it does not eliminate the risk of compromise. Responsible entities should deploy endpoint detection and response (EDR) capabilities across both IT and OT environments to detect adversary activity that bypasses or circumvents segmentation controls.

Recommend identity-based segmentation approaches as a complement to network-based segmentation. Modern zero-trust architectures that enforce access controls based on verified identity and device posture management, combined with just-in-time identity application can provide much more granular and adaptive segmentation than traditional network-based approaches, particularly in dynamic cloud and hybrid environments. Effective application of zero-trust principles are proven to radically reduce or prevent lateral movement, and privilege escalation during a compromise. Zero-trust principles also complement the phishing-resistant MFA requirements and would further strengthen the identity posture in the proposed amendments.

Cyber 3: Multi-Factor Authentication (MFA)

The proposed amendments require CI entities to implement phishing-resistant MFA across critical systems, and complement it with centralised logging, monitoring and review of authentication activity. The provision aims to strengthen identity security as a core control for protecting critical systems and access pathways.

CrowdStrike strongly supports the proposed requirement for deploying phishing-resistant MFA across online and internet-facing networks, critical systems, and remote access. Compromised credentials remain one of the most prevalent initial access vectors in cyber incidents affecting CI, and phishing-resistant MFA is one of the most effective controls available to entities for mitigating this risk. CrowdStrike's threat intelligence data confirms

that adversaries have developed sophisticated techniques for bypassing traditional MFA implementations, including SIM swapping, MFA fatigue attacks, and adversary-in-the-middle phishing frameworks.

Recommendations

Provide clear guidance on what constitutes 'phishing-resistant' MFA in the context of the CIRMP Rules. The Department should provide guidance specifying that SMS-based one-time passwords and push notification-based MFA do not meet the phishing-resistant standard, and should identify the specific authentication methods that do qualify.

Address the specific challenges of MFA implementation in OT environments, where legacy systems and operational constraints may make standard MFA implementations impractical. The guidance should provide alternative compensating controls for environments where phishing-resistant MFA cannot be directly implemented, such as privileged access workstations, jump servers with strong authentication, and enhanced monitoring of privileged access sessions.

Enhance phishing-resistant MFA requirements with additional Identity Threat Detection and Response (ITDR) and logging requirements. Threat actors exploit resulting gaps and weaknesses from traditional authentication methods. Emerging identity-centric approaches to security defeat these threats using a combination of real-time authentication traffic analysis, telemetry from endpoints, zero-trust principles, and machine learning analytics to quickly identify and prevent identity-based attacks.

Cyber 4: Enhancing Cyber Material Risks

The amendments expand the definition of cyber 'material risks' by requiring entities to explicitly address a broader set of failure and risk scenarios as identified by the Department of Home Affairs. This could include unsupported or unpatched systems, legacy and obsolete technology, risks from deploying or being targeted by emerging technologies, and offshore remote access to operational technology systems and business-critical data.

CrowdStrike strongly supports the requirement for CI entities to consider and mitigate the risks of legacy systems. The inclusion is a pragmatic and necessary addition to the CIRMP framework that reflects an important operational reality for many CI operators. Legacy OT systems in particular often cannot be patched or updated, creating persistent vulnerabilities that adversaries can exploit. This could be further supported by developing a 'legacy system risk management' framework that provides responsible entities with a structured approach to assessing, prioritising, and mitigating risks from unsupported and end-of-life components.

Recommendations

Provide specific guidance on AI risk management for CI entities, including that the use of AI for cybersecurity defence is not considered to be a high-risk application of AI. The

inclusion of AI as a specific material risk category is particularly timely and important. CrowdStrike has documented the rapid adoption of AI capabilities by adversaries to enhance the speed, scale, and sophistication of their operations. In today's threat landscape, defending against AI-accelerated adversaries, and securing AI systems themselves, requires cybersecurity operating at machine speed. The CIRMP should clearly distinguish between higher-risk, general-purpose AI uses and the deployment of AI for cybersecurity defence. Instead of applying broad restrictions that could unintentionally slow defenders, the policy should take a risk-based, outcomes-focused approach that encourages CI entities to deploy AI safely to strengthen their detection, response, and recovery capabilities.

Explicitly define business critical data to exclude data used for cybersecurity purposes. Such a clarification helps avoid inadvertent impacts on CI entities' ability to conduct state-of-the-art cybersecurity. Forcing the localisation of data for cybersecurity purposes threatens entities ability to manage cybersecurity risk. It reduces the ability of organizations to identify, protect, detect, respond, and recover in the face of cyber-attacks, and makes it impossible to implement best cybersecurity practices, and frameworks, such as MITRE ATT&CK.

V. CONCLUSION

CrowdStrike commends the Australian Government for its ambitious and intelligence-led approach to enhancing the CIRMP Rules. The proposed amendments reflect a sophisticated understanding of the contemporary threat landscape and represent a meaningful step forward in Australia's CI security framework.

CrowdStrike stands ready to support the Department, responsible entities, and the broader Australian CI community in implementing these enhancements. Our threat intelligence, incident response experience, and security technology capabilities are directly relevant to the challenges that responsible entities will face in achieving compliance with the enhanced requirements, and we welcome the opportunity to contribute to Australia's national resilience.

We welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

VI. 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/.

***