REQUEST FOR COMMENT RESPONSE

CrowdStrike Response to the Department of Home Affairs Consultation Paper: Proposed Amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018

1 May 2026

I. INTRODUCTION

CrowdStrike welcomes the opportunity to provide input on the Department of Home Affairs' Consultation Paper on proposed amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018 (SOCI Act). 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. This operational experience gives CrowdStrike a unique vantage point from which to contribute to the amendments to the Ministerial Directions Powers.

II. COMMENTS

CrowdStrike's 2026 *Global Threat Report*, and ongoing threat intelligence operations, confirm that nation-state adversaries are actively pre-positioning within CI networks including actors such as VANGUARD PANDA (VOLT TYPHOON), and AQUATIC PANDA (SALT TYPHOON).[1] There is a strong focus amongst these actors in compromising national CI, including telecommunications, energy, water, and transportation sectors. These actors prioritise persistence and stealth over immediate disruption, seeking to establish footholds that can be activated during periods of geopolitical tension or conflict.

If implemented with strong safeguards, clear thresholds, and clear alignment with risk-management approaches, these reforms will improve the Government's ability to manage systemic and emerging risks; strengthen public-private coordination; and achieve improved security outcomes across CI sectors without adding to the unnecessary complexity and duplication identified in the Independent review.

[1] *CrowdStrike 2026 Global Threat Report*, https://www.crowdstrike.com/en-us/global-threat-report/.

Measure 2 — 'Conditions' Power

The Independent Review recommended the development of earlier and more flexible Ministerial intervention tools. The draft amendments introduce a new power allowing the Minister to impose tailored, ongoing 'conditions' on entities to manage governance, access, and security risks, including FOCI-related concerns under the Foreign Acquisitions and Takeovers Act (1975) (FATA). It provides a more precise and proportionate alternative to blunt directions, particularly for persistent or structural risks.

Our experience in supporting CI operators with their security programs confirms that governance-level vulnerabilities are among the most difficult to detect and remediate. Unlike vulnerabilities which can be detected through technical means, governance vulnerabilities can be deeply embedded in corporate structures, contractual arrangements, and organisational culture.

CrowdStrike supports the introduction of a dedicated conditions power with appropriate safeguards. The ability to impose targeted, ongoing governance conditions on CI entities where ownership, control, or governance arrangements create a material national security risk is an important and necessary addition to the regulatory toolkit as noted in the Independent Review.

CrowdStrike supports the inclusion of cybersecurity baseline and uplift conditions among the illustrative examples of conditions that could be imposed. Implementing privileged access management, continuous monitoring and logging, and secure remote access arrangements are foundational security controls that CrowdStrike consistently recommends.

Recommendations

Develop technically rigorous, outcome-based cybersecurity baseline standards for use in conditions directions, in collaboration with the Australian Cyber Security Centre (ACSC) and industry. These standards should be regularly updated to reflect the evolving threat landscape and should be technology-neutral to avoid mandating specific products or architectures.

Publish clear guidance on the SOCI-FATA interaction. This should include the criteria for determining which legislative pathway is most appropriate for the threat being addressed where both frameworks may apply, and the process for coordinating between the Minister for Home Affairs and the Treasurer.

Ensure conditions in Ministerial Rules are proportionate and targeted to the identified risk. The legislation should include an explicit requirement that Ministerial Conditions be no broader than necessary to mitigate the identified risk, and that the Minister consider less intrusive alternatives before imposing conditions. This is consistent with the safeguards

already proposed in the consultation paper and should be reflected clearly in the legislative text.

Provide for independent technical assessment where conditions relate to cybersecurity controls or technical architectures. The Department should consider establishing a mechanism for independent technical experts including from the private sector to advise on the appropriateness and feasibility of proposed technical conditions before they are imposed.

Include impacted entity in sunset and review process. The proposed requirement for the Minister to review conditions directions within 12 months of issue, and at least every 24 months thereafter is an important safeguard against conditions becoming entrenched beyond their operational necessity. We recommend that this review process also include a formal mechanism for affected entities to provide evidence of changed circumstances that may warrant variation or revocation of conditions, and that the Minister be required to respond to such representations within a defined timeframe.

III. Cross-Cutting Recommendations

Government-Industry Information Sharing

The effectiveness of the proposed directions powers will depend significantly on the quality and timeliness of threat intelligence shared with affected entities. Entities cannot effectively comply with directions or take proactive steps to mitigate risks before directions are issued if they do not have adequate visibility into the threats they face.

CrowdStrike recommends that the Department, in conjunction with the ACSC, develop enhanced mechanisms for sharing threat intelligence with CI entities and their key security vendors. This should include:

- Classified threat briefings for security-cleared personnel at CI operators and their key security vendors, to provide context for directions and enable more effective compliance planning;
- Unclassified threat advisories that can be shared more broadly within affected organisations and with their broader supply chain partners; and
- Expanding sector-specific threat intelligence sharing forums, building on existing SOCI Act mechanisms.

Outcome-Based Direction Design

CrowdStrike strongly recommends that directions issued under the proposed powers be designed to specify security outcomes and risk thresholds, rather than mandating specific technical controls or architectures. Technology-prescriptive directions risk becoming outdated as the threat environment evolves and as new security technologies emerge, or to be ineffectual in a CI entities' individual environment. Outcome-based directions provide entities

with the flexibility to implement the most effective available controls while ensuring that the underlying security objective is achieved.

Where directions do reference specific technical controls, for example, as part of compensating control requirements under Measure 3, these should be drawn from recognised, regularly updated and appropriately standards wherever possible rather than being specified in the direction itself.

Regulatory Coherence and Cumulative Burden

CrowdStrike recommends that the Department conduct a comprehensive regulatory mapping exercise to identify potential overlaps, conflicts, and cumulative burden issues arising from the proposed reforms, and develop guidance to help entities manage their obligations in an integrated and efficient manner. CI entities are subject to an increasingly complex and overlapping set of regulatory obligations. The proposed reforms have the potential to add further layers to this regulatory landscape. This is particularly important for entities that are subject to both SOCI Act obligations and FATA conditions, where the interaction between the two frameworks may create compliance complexity.

International Alignment

CrowdStrike recommends that the Department actively engage with Five Eyes partners and other allied nations to promote alignment of CI security frameworks, including vendor risk management approaches, incident reporting requirements, and supply chain security standards. Australia's CI security framework does not operate in isolation. Many CI operators are multinational entities subject to security requirements in multiple jurisdictions, and the supply chains that underpin Australian CI are globally integrated. Aligned frameworks reduce compliance burdens for multinational operators, strengthen collective resilience against shared threats, and reduce the risk of adversaries exploiting regulatory gaps or inconsistencies between jurisdictions.

IV. CONCLUSION

CrowdStrike commends the Australian Government for its proactive and consultative approach to strengthening the CI security framework. We welcome the opportunity to discuss our submission in further detail with the Department and are available to provide technical briefings on any of the issues raised in this response. Public policy inquiries should be made to:

[redacted]

[redacted]

Email: policy@crowdstrike.com

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/.

***