REQUEST FOR COMMENT RESPONSE

Streamlining and Modernising the Security of Critical Infrastructure Act 2018

31 July 2026

I. INTRODUCTION

In response to the Department of Home Affairs request for feedback on proposed Tranche 2 reforms to the *Security of Critical Infrastructure Act 2018* (SOCI Act) CrowdStrike offers the following views.

We approach these comments as a leading international, U.S.-headquartered, cybersecurity provider that defends enterprises from globally distributed threats. Our AI-powered, cloud-native platform delivers state-of-the-art, real-time detection, automated protection, and threat intelligence across endpoints, cloud, identity, data, and AI workloads. Our insights are informed by applied, real-world experience across global industries through our software-as-a-service cybersecurity platform, incident response, managed threat hunting, and managed security services. CrowdStrike's recommendations are grounded in this operational experience.

II. COMMENTS

We appreciate the Department of Home Affairs' efforts to improve the cybersecurity practices of Australian critical infrastructure entities.

CrowdStrike supports the consultation paper's overarching goal of better protecting Australia's critical infrastructure, and the citizens who depend on it, from cybersecurity threats. These threats continue to evolve and grow more severe. As illustrated in CrowdStrike's 2026 Global Threat Report[1] government agencies and related entities remain top targets for cyber attacks. Nation-state adversaries continue to leverage stealth and scalable techniques to collect targeted surveillance data, strategic intelligence, and intellectual property. This makes steps to enhance cybersecurity across critical infrastructure sectors timely and appropriate.

We do not have feedback on every aspect of this consultation paper, but we do want to offer several points that may be of value to the Department as it finalises the legislative

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

package.

III. RECOMMENDATIONS

A. AI-Enabled Cybersecurity: A Note on the Role of Technology

Across several of the proposed measures including Measure 5 (cyber security incident definition), Measure 19 (supply chain cyber security), and Measure 15 (CIRMP assurance), the consultation paper appropriately recognises that AI-enabled systems are changing the nature of both cyber threats and cybersecurity responses. CrowdStrike wishes to highlight one important corollary to this observation: AI is also a critical part of the solution, not only a source of new risk.

The use of AI to detect cyber threats is an enormous advantage. Today, security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments, and AI can help defenders process this data and make detections more actionable. Sophisticated security teams are leveraging AI to eliminate some of the biggest bottlenecks in security operations including triaging alerts, malware analysis, and threat hunting. This scales expertise, drives consistent outcomes, and allows operations to act at machine speed. Leveraging best-in-class cybersecurity technologies deploying AI is essential to meeting constantly-evolving threats.

As the Department continues to develop the SOCI framework and supporting Rules, CrowdStrike recommends that the regulatory design actively accommodate, and where possible incentivise, the adoption of AI-powered security technologies by critical infrastructure operators. Given the uneven cybersecurity capacity across the regulated community, managed security services and AI-enabled security tools are among the most efficient pathways for smaller or less-resourced critical infrastructure operators to achieve meaningful security uplift. Policymakers should consider mechanisms to further incentivise adoption across the community.

B. Measure 1 — Exemptions Framework

CrowdStrike supports the proposed establishment of a single, consolidated exemptions framework to provide targeted relief where another Commonwealth, State, Territory, or recognised framework delivers substantially equivalent or stronger outcomes for the same asset, entity, function, or risk. Where appropriate, the exemptions framework and its supporting criteria focus on principles rather than prescriptive requirements and include a mechanism for periodic review, updates, and revisions.

C. Measure 8 — Data Storage or Processing Capture Pathways

CrowdStrike supports the proposed replacement of the current customer-driven capture model with a multi-pathway, operator-facing framework. The Department should ensure that its capture model reflects contemporary cloud operating models.

D. Measure 19 — Supply Chain Cyber Security Assurance

CrowdStrike supports the proposed clarification of CIRMP expectations for cyber security assurance of major suppliers.

Efforts to address supply chain cyber security should cover proactive operations seeking to disrupt adversary infrastructure and dependencies, rather than waiting to do so in response to a major incident. Supply chain disruption activities should be aligned to coordinated law enforcement actions where possible, and broader diplomatic and defence activities where appropriate.

As adversaries continue to evolve and refine their tactics, organizations must increase their emphasis on modern cybersecurity practices that leverage the most effective technologies. Guarding against current cyber threats requires continual innovation so national protections remain both resilient and effective. To defend against increasingly sophisticated adversaries, current best practice for organisations includes:

- **Endpoint Detection and Response (EDR):** EDR solutions defend endpoints such as desktops, laptops, servers, mobile devices, and cloud workloads from malicious activity. EDR provides granular visibility of potential threats. This enables holistic, real-time threat detection and proactive threat prevention. Leveraging EDR, defenders can perform threat hunting, incident response, and a variety of other essential cybersecurity tasks. EDR capabilities are a core pillar of most contemporary sophisticated security programs.

- **Cloud Security**: Leveraging cloud systems provides numerous operational efficiencies and security enhancements. Given today's rapidly evolving threat landscape, organizations must address cloud-specific and cross-domain threats (where adversaries traverse cloud and on-premise environments). Security teams must protect data, manage identity and access, and hunt for and respond to threats in real-time. Capabilities of particular relevance include cloud workload protection, cloud-native application protection

platform (CNAPP), cloud security posture management (CSPM), and Software-as-a-Service (SaaS) security.

- **Next-Generation Security Information and Event Management (SIEM) solutions:** Sophisticated threats mean that modern enterprises must achieve visibility, context, and protection across systems and resources, including cloud and ephemeral resources. This often implies the need for multiple security and monitoring tools or capabilities. Next-Gen SIEM solutions leverage rich endpoint telemetry (like that captured by Endpoint Detection and Response [EDR] tools) and integrate it with other security-relevant event information from an array of sources. Supported by AI, this provides defenders a more coherent view, intuitive workflows, and ultimately better control of their environments.

- **Artificial Intelligence-Based Prevention**: The core of modern cybersecurity solutions is the ability to prevent zero-day attacks and malware-free attacks, and achieve visibility across environments. Machine learning and artificial intelligence are essential to this end. Leveraging these technologies is essential to meeting constantly-evolving threats.

- **AI Detection and Response (AIDR)**: Security teams increasingly require specialized capabilities to protect the enterprise throughout the AI lifecycle. An emerging security category called AIDR enables security teams to: monitor AI behavior and interactions; secure AI agent identities and access; discover shadow AI; prevent sensitive data leakage to AI systems; protect cloud-based AI applications; and implement guardrails on AI system actions.

- **Identity Threat Detection and Response (ITDR):** As organizations increase deployment of cloud services, work from anywhere models, and Bring-Your-Own-Device policies, enterprise boundaries continue to erode. Threat actors exploit resulting gaps and weaknesses from traditional authentication methods. In fact, compromised valid identities are a common initial access vector in incidents. However, emerging identity-centric approaches to security defeat these threats using a combination of real-time authentication traffic analysis, telemetry from endpoints, and machine learning analytics to quickly identify and prevent identity-based attacks.

Additionally, there are multiple security program requirements that bolster 4

organizations' security posture:

- **Threat Hunting**: Whether through supply chain attacks or otherwise,

adversaries periodically breach even very-well defended enterprises. However, skilled defenders can find them and thwart their goals. Proactive hunting is a leading indicator of the strength of an enterprise cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. The more well-instrumented the environment, the more opportunities defenders give themselves to identify malicious activity as an attack progresses through phases. Optimally defenders or their service providers continually hunt for threat activity 24/7, 365 days per year.

- **Zero Trust Architecture:** Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate security protections focused on identity and authentication. By eliminating transitive trust, Zero Trust Architecture concepts radically reduce or prevent lateral movement and privilege escalation during a compromise. This constrains threat actors' ability to achieve actions on objective and provides additional opportunities for defenders to detect threats.

- **Logging Practices**: Organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases.

- **Managed Security Service Providers**: Some entities lack the cybersecurity maturity to run effective security programs internally, or lack the scale to support a robust, 24/7, 365 days per year security capability. Increasingly, such entities should rely upon managed service providers, which can be more efficient overall and enable organizations to apply internal IT/security resources toward domain-specific challenges, including governance, risk, and compliance. Adopting an MSSP can radically strengthen organizations' security posture.

IV. CONCLUSION

CrowdStrike appreciates the Department of Home Affairs' continued engagement with industry stakeholders on these important reforms. We reiterate that continued

engagement with industry is essential, given the important role the private sector plays in this effort.

Because the underlying technologies evolve faster than law and policy, we recommend

the Department continue to focus on principles rather than prescriptive requirements throughout the final legislative package and conduct regular updates to the framework as the threat environment and technology landscape develop.

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.

CrowdStrike: We stop breaches.

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

VI. CONTACT

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

Drew Bagley Brian Fletcher
Chief Privacy and Policy Officer Director Public Policy APJ Email:

policy@crowdstrike.com

***