REQUEST FOR COMMENT RESPONSE

HORIZON 2 DISCUSSION PAPER ON AUSTRALIA'S NATIONAL CYBER SECURITY STRATEGY

29 August 2025

I. INTRODUCTION

CrowdStrike appreciates the opportunity to provide our comments to the Department of Home Affairs ("Home Affairs") on the Horizon 2 Discussion Paper on Australia's National Cyber Security Strategy[1]("Horizon 2"). CrowdStrike previously provided comments on the National Cyber Security Strategy, most recently on the Legislative Reforms Consultation Paper in March 2024.[2]

CrowdStrike is an international cybersecurity company based in the United States that helps protect businesses around the world from globally-distributed cyber threats. We have extensive experience helping organizations 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

CrowdStrike (CRWD) supports the Australian Government's aim under Horizon 2 to elevate national cyber defences. The Strategy's emphasis on proactively addressing cyber threats, continued stakeholder collaboration, and mitigating risk as a shared responsibility, is timely and important. We see the most important outcomes to be:

1) more collaboration with Government recognizing that 'industry expertise' is vital and that 'genuine partnerships' are needed for enduring solutions;

2) more security-conscious citizens and businesses, rightly framing cybersecurity as a shared responsibility across the digital economy;

3) streamlined regulatory expectations, which will make it easier for Australian businesses to invest in security capabilities rather than in compliance tasks; and

[1] Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy[2] 2025 Threat Hunting Report | Latest Cybersecurity Trends & Insights | CrowdStrike

4) a recognition that cybersecurity underpins sovereignty and national growth by enabling Australian businesses to scale globally, attract investment, and benefit from Australian innovation.

1. What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?

The 2025 CrowdStrike Threat Hunting Report[3] highlights the accelerating pace and sophistication of cyber threats. Adversaries are increasingly relying on advanced techniques such as identity-based attacks and malware-less intrusion methods that bypass traditional defences. These trends reinforce that threat levels will continue to rise in both scale and complexity.

To counter these developments, Australia must adopt modern and scalable approaches to cybersecurity. Static, perimeter-based defences are no longer sufficient. Cloud-native, AI-driven platforms that integrate detection across endpoints, identities, cloud workloads, and unmanaged devices represent best practice. This will ensure Australia's cybersecurity ecosystem keeps pace with adversary innovation.

Policymakers should recognise that large, diverse datasets created through secure and lawful cross-border flows are central to strengthening AI-driven defences capabilities. The report illustrates how adversaries leverage global infrastructure making cyber threat data sharing across borders critical. Localised data sets, siloed within national boundaries, will become increasingly ineffective against adversaries who operate globally. Similarly the report describes the speed with which attackers are exploiting vulnerabilities. Artificial intelligence will play a decisive role for defenders to address this speed of compromise. Cloud-based AI solutions enable real-time detection, rapid response, and innovation at scale.

The private sector plays an increasingly critical role in delivering advanced cybersecurity capabilities to Australia, including to small and medium enterprises in critical sectors. Access to products and services delivered by the private sector including cloud-based endpoint detection and response capabilities that operate at national scale, threat intelligence, and proactive threat hunting ensure that the benefits of cutting-edge security are not confined to the largest corporations or government agencies. By embedding partnerships with the private sector into the national strategy,

[3] 2025 Threat Hunting Report | Latest Cybersecurity Trends & Insights | CrowdStrike

Australia can accelerate the diffusion of advanced cybersecurity approaches and rapidly raise baseline cybersecurity across the economy.

Speed to respond

One continuing trend is the speed by which adversaries are able to compromise victim organisations after achieving initial access to the IT environment. Adversaries work rapidly at the outset of breach and they are constantly reducing how long it takes for them to move laterally and gain privileged access to the environment. Once they have that, they can gain access to even more systems and data, and stay in the organisation's IT environment for as long as it takes for them to achieve their objectives.

This means when responding to a potential security incident or event, every second counts. The faster defenders can detect an attack, the better the chances that response activities will prevent adversaries from achieving their objectives.

Modern cybersecurity approaches

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 defends endpoints such as desktops, laptops, servers, mobile devices, and cloud workloads from malicious activity. It provides granular visibility of potential threats and gives defenders the ability to conduct real-time threat detection, proactive threat prevention, threat hunting, incident response, and a variety of other essential cybersecurity tasks in their IT environment. EDR capabilities are a core pillar of most contemporary sophisticated security programs.

Cloud Security: Leveraging cloud systems provides both operational efficiencies and security enhancements for organisations over legacy infrastructure. In cloud environments, security teams can protect data, manage identity and access, and hunt for and respond to threats in real-time.

Next-Generation Security Information and Event Management (Next-Gen SIEM): Sophisticated threats mean that visibility, context, and protection across all systems

and resources, including cloud and ephemeral resources is essential. Next-Gen SIEM solutions leverage rich endpoint telemetry (like that from EDR) and integrate it with other security-relevant event information. Supported by AI, this provides defenders a

more comprehensive view of their environment, and allows for more intuitive security workflows. This ultimately gives them better control of their environments and leads to more effective security outcomes for organisations.

Machine Learning-Based Prevention: The core of all modern cybersecurity solutions is the ability to defeat novel threats based on behavior cues rather than known software signatures. Machine learning and artificial intelligence are our best chance of detecting constantly-evolving threats and leveraging these technologies is essential to effective cybersecurity outcomes.

Identity Threat Detection and Response: As deployments of cloud services, work from anywhere models, and Bring-Your-Own-Device policies increase, the traditional concept enterprise boundaries continue to erode. Threat actors are exploiting gaps and weaknesses that arise from traditional authentication methods trying to work across these new extended environments. Compromised valid identities are an extremely common initial access point for adversaries. 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 these identity-based attacks.

Threat Hunting: Due to the sophistication and ability to innovate of many of the modern cyber adversaries, defenders should periodically search inside their environment for adversaries as part of a multilayered security approach. Proactive threat hunting is a leading indicator of the strength of an enterprise cybersecurity program.

Zero Trust Strategies: Zero Trust is a modern security approach that assumes no user, device, or application is trusted by default. This approach is critical against today's adversaries, who routinely exploit stolen credentials, supply-chain weaknesses, and remote access to bypass traditional perimeter defenses.

Logging Practices: Whilst not a new security approach, it is increasingly important that organisations collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases.

2. Are there initiatives or programs led by State or Territory Governments you would like to see expanded or replicated across other levels of government?

One-way CrowdStrike supports state and local governments in the United States is by

providing ways to take a whole-of-state approach to cybersecurity. CrowdStrike provides a framework that enables states to extend advanced cybersecurity protections beyond central IT environments to all levels of government, including municipalities, school districts, and smaller agencies that often lack the resources to deploy modern security on their own.

By standardising tools and practices, a whole-of-state security approach helps create a more consistent security posture across diverse public sector organisations, reducing fragmentation and ensuring that smaller entities benefit from the same protections as larger ones.

The program promotes coordinated threat detection and response across entire states. Rather than leaving individual agencies or local governments to face sophisticated adversaries in isolation, the whole-of-state security approach scales advanced cybersecurity capabilities such as threat intelligence, monitoring, and response activities across multiple government entities.

This collective approach improves state-wide resilience and enables state governments to manage incidents at scale.

III. SHIELD 1: STRONG BUSINESSES AND CITIZENS

A strong national cybersecurity posture depends on ensuring that businesses and citizens can both access and implement effective protections. This requires a regulatory environment that promotes best practice while avoiding unnecessary complexity.

We support the Australian Government's ambition to provide greater regulatory clarity while setting high standards for cybersecurity. Regulatory efficiency is not about lowering standards, but about ensuring that rules remain coherent, outcomes-focused, and aligned across jurisdictions. Harmonised and simplified cyber regulations lowers compliance costs from duplication, and makes it easier to focus resources on improving security outcomes rather than navigating inconsistent rules.

It is important that these rules are practical, outcomes-focused, and internationally aligned making consultation with industry essential. Interoperable rules enable Australian businesses to operate securely and competitively in international markets.

Australia can strengthen cyber resilience across the entire economy and community and governments at all levels have a direct role to play in this. Federal and state governments can support local governments, often the least resourced but most targeted, with innovative approaches such as whole-of-state cyber solutions or

centrally supported shared services. Model architectures and trusted environments supported by Government can encourage the growth of a local security services ecosystem, and help not-for-profits and SMEs access high-quality security services.

5. *What could Government do to better target and consolidate its cyber awareness message?*

Government can improve the targeting and consolidation of its cyber awareness messaging by grounding it in a simple, principle-based framework that is widely recognised and easy for all stakeholders to understand. Simplified, principle-based guidance gives organisations practical flexibility to implement security in ways that suit their environments, without being constrained by overly prescriptive rules.

Shaping cyber awareness messaging by using the highest-level of models such as the NIST Cybersecurity Framework, or an Australian equivalent aligned with it helps citizens and businesses focus on a few core cybersecurity principles, such as identify, protect, detect, respond, and recover (from the NIST Cybersecurity Framework). This provides a national common language for messages that can be applied across sectors and organisation sizes, and from all levels of government. Anchoring communications in such a framework reduces complexity and helps avoid conflicting advice that can arise when navigating a patchwork of overlapping messages.

Building awareness around broad, consistent principles also makes it easier to tailor messages for different audiences. Whether directed at small businesses, local governments, or individual citizens, the same foundational framework can be applied in plain language and illustrated through practical examples. This approach simplifies communications while raising the baseline of understanding, and it ensures alignment with international best practice so Australia remains globally competitive.

10. *What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from Government would have the most impact in the NFP sector?*

Skills and funding are critical enablers of stronger cybersecurity for not-for-profits, which often operate essential community services on very limited budgets. Government can help by funding a program for trusted cybersecurity companies to

provide security services to NFPs. This extends advanced capabilities such as monitoring, detection, and response capabilities to organisations that cannot resource these functions themselves, and ensures consistency with national best practices.

This ensures an essential Australian sector is not left behind in the national resilience effort. NFPs gain access to advanced cyber capabilities without the expense of building an in-house team.

12. *How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing?*

Ransomware remains one of the most significant cyber threats facing individuals and small organisations, and its impact continues to evolve. Traditional malware-based ransomware has increasingly been replaced by malware-less techniques such as credential theft and identity-based intrusion, which allow adversaries to move quickly and often undetected. CrowdStrike threat hunting data shows that hands-on-keyboard intrusions are rising year-on-year, with attackers now able to move from initial access to ransomware deployment in less than 24 hours. These techniques pose particular challenges for smaller entities and individuals who may lack the resources to detect and respond at speed.

Ransomware will continue to adapt, but a focus on identity security, rapid detection, and resilience can blunt its impact across the economy. The continuing evolution of ransomware also highlights the need to shift from static, prevention-only approaches to modern, scalable solutions that integrate detection, response, and resilience. Cloud-native tools such as EDR and managed threat hunting allow organisations of all sizes to defend against and adapt to changes in the behaviour of the most sophisticated adversaries. For small entities and individuals, guidance and support from government and trusted providers can help bridge the resource gap.

Building resilient-by-design businesses is also essential in the face of the ransomware threat. Organisations should be supported to conduct risk assessments, prepare for incidents, and recover quickly, recognising that some level of exposure is inevitable.

Our most recent information on the ransomware threat, and cyber threats and intrusions more broadly can be found in the CrowdStrike 2025 Global Threat[4], and 2025 Global Threat Hunting[5] Reports.

[4] 2025 Global Threat Report | Latest Cybersecurity Trends & Insights | CrowdStrike [5] 2025 Threat Hunting Report | Latest Cybersecurity Trends & Insights | CrowdStrike

13. *How could the government further support businesses and individuals to protect themselves from ransomware attacks?*

Ransomware has been one of the most persistent and damaging cyber threats for several years, impacting individuals, businesses, and governments alike. The Australian

Government should consider the full range of tools available to it—policy, regulatory, diplomatic, intelligence, and law enforcement—to push back against this difficult and evolving threat. A coordinated national approach that combines domestic measures with international action is essential to disrupt ransomware actors and reduce their ability to operate with impunity.

One way the Government can further support businesses and individuals against ransomware by remaining actively engaged with international initiatives such as the Counter Ransomware Taskforce. Ransomware is a transnational crime that exploits global infrastructure, and sustained international collaboration is critical to disrupt attacker ecosystems, trace illicit financial flows, and impose costs on adversaries.

Domestically, the Government can strengthen resilience by promoting modern security practices such as identity protection, rapid detection, and incident response through simple, principle-based guidance aligned with international frameworks. Targeted support for small organisations, not-for-profits, and local governments is especially important, as these entities often lack resources but remain frequent targets. By combining international cooperation with local resilience measures, the Government ensures Australians are better protected across all levels of the economy.

16. Which regulations do you consider most important in reducing overall cyber risk in Australia?

The 2023–2030 Cyber Security Strategy, Government initiatives such as the voluntary Cyber Health Check program provide an important baseline for SMBs to assess their security posture and understand what is possible. By making practical tools and diagnostics available at little or no cost, these programs help businesses that lack in-house expertise understand their risks and take initial concrete steps toward strengthening their defences. Importantly, such programs complement regulatory approaches by ensuring that SMEs are not simply left with obligations, but also with accessible pathways to compliance and resilience.

Over time, embedding cyber health checks into normal business practice normalises continuous improvement, rather than treating cybersecurity as a one-off exercise.

With targeted funding and private sector partnership, these programs can evolve into a trusted ecosystem of support for SMBs that strengthen the entire Australian economy.

III. SHIELD 2: SAFE TECHNOLOGY

Policies that prioritise strong cybersecurity are fundamental to protecting Australia's

most valuable datasets and sustaining digital sovereignty. Cybersecurity risk does not sit only in systems or networks, but in the confidentiality, integrity, and availability of data itself. By focusing on protecting the data rather than only its physical location, the Government can best safeguard sensitive information.

Government should also encourage the adoption of modern cybersecurity technologies and strategies. Cloud-native and AI-enabled solutions already deliver world-class capabilities at scale and give Australian organisations access to defences that evolve as fast as adversaries do. Promoting best practice frameworks and incentivising their uptake ensures that all organisations, including SMEs and not-for-profits, can protect themselves effectively.

The Government should also strengthen communication of threats so business leaders can make the best informed decisions about managing their cyber risks. Clear, principle-based risk communication—grounded in internationally aligned frameworks—help businesses, governments, and citizens reduce their exposure to cyber threats.

18. *What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, CER and operational technology?*

Australia should ground its secure technology standards and frameworks in internationally recognised models. Adopting global standards allows Australia to take advantage of investments already made elsewhere, avoid duplication, and ensure local businesses can scale confidently into international markets. This principle of interoperability—rather than creating unique local requirements—reduces cost, improves efficiency, and strengthens sovereignty by giving Australian organisations access to the best available protections.

Operational technology (OT) requires special consideration. OT cybersecurity is one of the most difficult disciplines to get right because traditional IT security concepts do not easily apply to industrial control, SCADA, or PLC systems. The best approach is to prioritise architectural mitigations—segmentation, specialised access controls, and

strict processes—while recognising that most attacks on OT originate from the compromise of enterprise IT networks. Defending enterprise environments robustly therefore provides the best chance to defend OT systems as well.

Standards for edge devices and to ensure critical entity resilience should reflect the same principles. Adopt risk-based, internationally aligned frameworks and

communicate requirements in a way that is simple, practical, and outcomes-focused to allow organisations to manage their own risk intelligently and innovate securely.

IV. SHIELD 3: WORLD-CLASS THREAT SHARING AND BLOCKING

Taking defensive action before incidents occur as part of a proactive cybersecurity posture is best practice around the world. Adversaries increasingly exploit speed and automation to compromise Australian networks and businesses should consume cyber threat intelligence to understand how the adversary will attempt to compromise them. By signalling clear support for proactive practices, the Government can drive a culture of continuous improvement rather than reactive compliance, and help organisations of all sizes shift resources toward prevention and resilience.

Government should actively encourage and enable the private sector to play a larger role in enabling and providing proactive strategies. Private companies hold unique visibility into threats across the global digital ecosystem. By encouraging industry to access timely threat intelligence and use threat hunting services, Australia as a whole can dramatically increase the effectiveness and timeliness of its defensive posture.

The Government should also empower the private sector to adopt the best available technologies and practices to deliver a national defensive posture that is fast, scalable, and proactive. Cloud-native, AI-driven solutions, backed by international standards, provide the speed and scalability required to confront modern adversaries. Providing guidance, incentives, and harmonised regulatory frameworks ensures that all sectors, from local government to national critical infrastructure, can apply the best technologies and services to defend against sophisticated threats.

Benefits to moving to the cloud include retiring legacy systems, operational improvements, improved resilience, and contracting efficiencies. Cybersecurity is core to modernising IT systems and innovation, and is part of the process. Driven largely by cloud SaaS offerings, IT resource consolidation has emerged as a theme in the cybersecurity industry and beyond. Across governments, this trend dovetails nicely with broader priorities to leverage 'shared services'-style acquisition models, which are more efficient, less costly, and more straightforward to administer and oversee.

24. *What could Government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry?*

Australia's proactive cybersecurity posture for industry should focus on prevention, resilience, and innovation. It should empower organisations to adopt cloud and AI-driven capabilities at scale, remove barriers that fragment global defences, and

encourage continuous collaboration between Government and the private sector. By embedding these principles, Australia can move decisively from a reactive model to one that anticipates threats, protects vulnerable data, and strengthens resilience across the entire economy.

As noted above, this includes encouraging the secure use of cloud services, which deliver scale, flexibility, AI-services and rapid innovation that on-premises solutions cannot match. Key to this is removing unnecessary data localisation requirements, as fragmented data rules reduce the effectiveness of modern, AI-driven defences that depend on global visibility and diverse datasets. Enabling lawful, secure cross-border data flows ensures that organisations can benefit from cutting-edge protections and remain competitive in global markets.

A proactive national posture also depends on fostering a vibrant domestic cybersecurity ecosystem. Government can strengthen this ecosystem by encouraging public–private partnerships, supporting start-ups and service providers that extend modern defences to SMEs and not-for-profits, and leveraging industry intelligence to improve national awareness. Promoting the adoption of modern, outcomes-focused approaches to cybersecurity such as cloud-based endpoint detection and response, identity protection, and continuous threat hunting allows organisations to anticipate and block threats before they cause harm.

25. *Does the Government need to scope and define what Australia's proactive cyber security posture should look like for industry?*

Government should scope and define Australia's proactive cybersecurity posture as a set of broad principles and outcomes rather than prescriptive rules. This approach creates a clear national direction while leaving space for Australian industry to innovate, adapt to emerging threats, and adopt the modern practices and technologies most suited to their environments and business models.

Internationally recognised frameworks such as the NIST Cybersecurity Framework demonstrate how this can be done: they provide simple, outcome-oriented categories

— identify, protect, detect, respond, recover — that guide organisations without constraining them. Adopting a similar model in Australia would ensure consistency, enable international interoperability, and give businesses the clarity they need to invest in innovation and resilience.

As a community, we should undertake a more serious conversation about expanding national Incident Response (IR) capacity. IR demand is incredibly elastic, and IR supply is relatively fixed. The best practice for private entities is to have an IR retainer in place,

so a skilled provider can offer specialised IR assistance within a stipulated time frame, and under other terms outlined in a Service Level Agreement (SLA).

A program, likely led by ASD, that retained skilled private sector providers in advance for use during significant cyber incidents would quickly expand the cybersecurity workforce on demand and strengthen national resilience. Eligibility for benefits under such a program could likely be based on need or vulnerability (e.g., for small businesses), and/or on criticality (e.g, entities with a national security nexus or critical infrastructure entities with systemic importance).

28. *What more is needed to support a thriving threat sharing ecosystem in Australia? Are there other low maturity sectors that would require ISACs, and what factors, if any, are holding back their creation?*

The Discussion Paper aligns with our belief that speedy info-sharing and co-action can greatly reduce harm during incidents.

A thriving threat-sharing ecosystem in Australia must recognise that the private sector produces world-class threat intelligence as part of a highly effective commercial model. Private companies invest heavily in collecting, analysing, and delivering this intelligence to customers, and that capability should be respected as an essential part of the national ecosystem. Government threat intelligence sharing policies should therefore remain voluntary. This ensures that commercial innovation in intelligence remains sustainable, while enabling collaboration where it benefits national resilience.

Government has a critical role in making more of its own intelligence available at lower classifications. Over-classification currently prevents timely and actionable use by industry and critical infrastructure operators. Government-industry collaboration provides the plausible cover to allow faster sharing of more information and at appropriate sensitivity levels. This type of release would significantly improve national resilience, without undermining the commercial threat intelligence market.

Certain low-maturity but high-risk sectors such as health, education, and not-for-profits would benefit from a formal Australian information sharing program.

To support their creation, Government can provide seed funding and trusted frameworks, while encouraging voluntary private sector participation. By combining voluntary industry contributions, a vibrant commercial threat intelligence market, and more open government sharing, Australia can strengthen the overall ecosystem and ensure that even vulnerable sectors gain access to actionable insights.

30. Are the roles and responsibilities of Government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?

Australia should aspire to a situation where Government and industry train, prepare, and respond as one team in times of crisis. Roles and responsibilities between Government and industry in a conflict or crisis scenario are improving but remain not fully clear. Questions persist around the legal protections available to companies if they must take defensive action in the national interest. This uncertainty risks slowing response at the very moment when speed matters most.

CrowdStrike strongly supports efforts to formalise collaboration between Government and industry, including the development of joint incident response playbooks and clear frameworks that define authorities, responsibilities, and protections. Safe harbour provisions that recognise the necessity of defensive action in a crisis also helps ensure industry can act decisively without fear of legal consequences when needed.

Government should continue to expand the scope and frequency of cyber exercises with private sector partners to build trust, clarify roles, and improve readiness to respond under pressure. Exercises provide the practical testing ground for joint playbooks, highlight gaps in communication or capability, and enable continuous improvement in national preparedness for all parties. Investing in regular, realistic, and inclusive exercises can ensure that both public and private parties are best prepared to respond quickly and effectively in a cyber conflict or crisis.

32. Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?

Australia should avoid replicating existing international mechanisms, but there is value in providing Australian researchers with a safe, clear pathway to report vulnerabilities. A national program could provide a trusted mechanism and establish legal clarity, while

leveraging existing global standards and models. This encourages responsible disclosure, reduces the risk of exploitation, and strengthens trust between researchers and organisations. Such a program should remain complementary to existing industry practices and commercial channels and not a replacement for them.

Within the private sector, longer-term vulnerability disclosure norms have emerged. These norms continue to evolve over time, and we anticipate additional changes as both developers and vulnerability researchers increasingly employ the assistance of artificial intelligence. We recommend Government align any vulnerability regulations

with these best practices; account for edge cases as is common in mature disclosure policies; and incorporate mechanisms for regularly updating policies.

V. SHIELD 4: PROTECTED CRITICAL INFRASTRUCTURE

Australia has a relatively mature regulatory framework for critical infrastructure (CI), but the cyber threat environment demands continuous uplift. Government should continue to strengthen this framework by ensuring that regulation remains outcomes-focused, harmonised across sectors, and internationally aligned. This reduces duplication, improves compliance efficiency, and gives CI operators the clarity they need to focus resources on security outcomes rather than administrative burdens.

Operators of CI must be empowered to adopt the best technologies and practices. Government should actively encourage the use of cloud-based, AI-enabled, and other modern security tools and strategies. Risk management education should be a central part of this empowerment, equipping boards, executives, and technical teams with the knowledge to make informed choices and build resilience-by-design ensuring Australia's CI remains secure, adaptive, and globally competitive.

The Australian Government should centralise risk management, security investment, and policy to drive uplift in the public sector. A coordinated approach avoids fragmentation, ensures consistent prioritisation of the most serious risks, and allows scarce resources and skilled personnel to be applied where they have the greatest impact. Centralisation also provides a platform for clearer communication between governments and industry, enabling faster collective responses to emerging threats.

33. How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?

The SOCI Act has played an important role in lifting the baseline of protection for Australia's CI and ensuring that operators take cybersecurity seriously. The obligations

have raised awareness and driven investment in risk management across essential sectors. However, the framework can be simplified and clarified to make it easier for operators to understand and implement their obligations.

In particular, it is important to emphasise that strong cybersecurity outcomes matter more than data localisation requirements. Mandates that focus on where data is stored or processed risk distracting from the more urgent task of protecting data through modern security controls. Clearer, outcomes-focused obligations—aligned with international standards—would ensure that CI operators can prioritise the technologies and practices that most effectively defend against advanced threats, while still meeting

regulatory expectations.

36. What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should Government play in enabling uplift, including through tools, guidance or incentives?

CI entities need clear guidance on adopting modern cybersecurity architectures and cloud-based solutions, with security considerations prioritised above all else. Government can play an enabling role by providing practical tools, reference architectures, and incentives that encourage IT modernisation and security at scale. As noted earlier, consolidating IT resources through secure cloud services allows operators to retire legacy systems, achieve holistic visibility, and embed stronger, more resilient security. Cybersecurity is a core element of this modernisation.

CI entities continue to struggle with securing critical supply chains, and compliance-based approaches alone have not materially strengthened their posture. A more effective and scalable approach is to incentivise small and medium suppliers in the CI ecosystem to adopt managed services, which promote information sharing and raise the baseline across the supply chain. Shared services and cloud-based acquisition models provide efficiencies for government and industry alike, while ensuring that advanced security tools are productised and easily consumable by users.

Industry needs to harness the benefits of AI-driven cybersecurity. AI is uniquely capable of defending against novel, malware-free attacks and processing the immense volume of telemetry from modern hybrid IT/OT environments. Government should support programs that deliver secure, cloud-enabled AI tools to CI operators in ways that deliver immediate time-to-value. By combining clear guidance, incentives for modernisation, supply chain uplift, and access to scalable AI-enabled services, Government can materially strengthen the operational resilience of Australian CI.

37. How can the Australian Government support private sector partners to better engage with Government security requirements, including certifications and technical controls?

Private sector partners can be supported to better engage with security requirements by aligning certifications and technical controls with internationally recognised standards, and providing risk, and principles-based security advice.

International standards and certifications provide consistency, reduce duplication, and allow Australian businesses to operate more effectively in global markets. They also ensure that security requirements are durable and adaptable as adversaries continue to innovate. A focus on risk-based controls with clearly defined outcomes make security

more practicable and enable companies to focus on the most important challenges.

Equally, Government should provide principle-based guidance that encourages the adoption of modern approaches to cybersecurity, rather than prescriptive checklists that quickly become outdated. Clear, outcome-oriented principles give organisations flexibility to adopt cloud, AI-enabled, and other advanced solutions that deliver stronger protection.

VI. SHIELD 5: SOVEREIGN CAPABILITIES

It is crucial for the continued growth of Australia's digital economy that "digital sovereignty" be framed in terms of having control and assured access to data and services, rather than mandating local data localization. The discussion paper recognises the need to manage Foreign Ownership, Control or Influence (FOCI) risks with a new vendor review framework – a sensible step to vet critical tech. Risk-based supply chain security is essential but should avoid policies that favours local data storage or excludes trusted global providers without cause.

Over-emphasizing localisation can backfire and effective security outcomes that ensure data is secure and accessible under Australian oversight provide much more assurance of sovereignty than physical location of servers. Research shows data localisation often fails to meaningfully improve security and instead increases costs and complexity . A constructive approach is to ensure Australia has 'sovereign control', meaning access to data under its laws when needed, diversity of supply options, and local talent development. This provides security without cutting off the benefits of global threat intel flows and best-in-class security technologies.

Threat detection efficacy depends on analysing telemetry across borders in real time. Closing off these flows weakens defences, as cyber adversaries operate globally and

adapt faster than any one nation's boundaries. Australia has traditionally supported open cross-border data flows in its trade policy, and this principle should carry through to the cyber strategy. The Government should explicitly support "data free flow with trust," ensuring that privacy and sovereignty measures are implemented with proper safeguards and supporting global threat intelligence and security technologies.

Horizon 2 can reconcile sovereign interests with the realities of a globally interconnected threat landscape, ensuring that Australian organisations retain access to cutting-edge defences and the intelligence required to stay ahead of adversaries.

44. How would we best identify and prioritise sovereign capabilities for growth and development across Government and industry?

To make the most of limited resources and achieve immediate gains, Government should prioritise capabilities that align with international frameworks, promote interoperability, and position Australia as a trusted partner in the global digital economy. The goal should be to strengthen capabilities that can scale across the broader global digital ecosystem, ensuring Australian companies can compete internationally while also contributing to national resilience.

To the extent that sovereign capabilities are required, Government should identify and prioritise areas that deliver genuine value-add rather than replicating what is already available globally. Skills and people are central to this effort. Investing in workforce development, research capacity, and public–private collaboration will do more to secure sovereignty than attempting to build duplicative technologies or mandating localisation.

Digital and cybersecurity policies must avoid sovereignty measures from becoming trade barriers. Harmonising domestic and global standards ensures that Australian companies can grow into export markets and participate in global supply chains without being locked out by unique local rules.

Government can learn from approaches taken by international partners where streamlining regulatory processes and digitising trade paperwork has enhanced both competitiveness and security. By applying similar principles, Australia can prioritise sovereign capabilities that strengthen its own digital ecosystem while ensuring that policies remain open, outward-looking, and supportive of long-term economic growth.

45. What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?

Organisations should seek to avoid overreliance on one vendor for separate enterprise IT functions to reduce concentration risk across their entire stack of IT technologies. This is something we see other countries looking at very closely.

In a modern enterprise environment, organisations have varying degrees of technology and vendor choice within their enterprise IT environment for functions such as operating system, office productivity suite, collaboration, browser, cloud, AI, and

security. Due to cost and operational efficiency benefits, organisations often assess that centralisation at any given layer of this (e.g. operating system, office productivity suite, or security) is appropriate.

Concentration of vendors across many or all layers in an enterprise's stack of technology choices is more problematic. It removes effective security boundaries, reduces opportunities for detection of malicious behaviour, enables threat actors' lateral movement/privilege escalation, and generally increases systemic risk. It is advised that organisations should introduce vendor diversity between disparate IT technologies in their environment where possible.

Cybersecurity policies should encourage risk-based procurement, and incentivise resilience measures such as layered defences and IT vendor diversification. Government should also avoid localisation mandates that inadvertently heighten concentration risk by shrinking the pool of available providers.

These approaches reduce systemic risk and strengthen Australia's ability to withstand supply chain and vendor-specific disruptions.

VII. SHIELD 6: STRONG REGION AND GLOBAL LEADERSHIP

Supporting neighbours to strengthen their cyber resilience reduces regional vulnerabilities and safeguards Australia's own economy and national security. Australia should prioritise regional cyber resilience and cooperation with partners across the Indo-Pacific to uplift cyber capacity, share threat intelligence, and build collective defences.

Equally, Australia must continue to shape, uphold, and defend international cyber and digital trade rules, norms, and standards. By promoting alignment and interoperability, Australia positions itself as a trusted partner and global leader in shaping the future and security of the digital ecosystem.

Open, trusted digital trade is central to Australia's economic future, and being an "open yet secure" digital economy will attract businesses and innovation. Australia should champion norms that support secure cross-border data flows, risk-based supply chain security, and principled state behaviour in cyberspace to ensure continued regional cybersecurity cooperation.

46. *Do you view attributions, advisories and sanctions as effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?*

Yes. Attributions, advisories, and sanctions are effective tools for countering malicious cyber activity. Public attribution helps raise costs for adversaries by exposing their methods and undermining plausible deniability, while advisories provide actionable information that enables defenders to protect themselves. Sanctions, when coordinated with partners, impose tangible consequences on malicious actors and their enablers. Together, these tools demonstrate that cyber operations carry risks and costs, not just rewards.

Australia should continue to work closely with trusted partners on coordinated attributions. Shared adversary taxonomies, such as those highlighted in CrowdStrike's work on strengthening global security, create a common language for understanding and communicating threats. This alignment enables faster collective responses, reduces ambiguity, and supports global deterrence.

The Government can also further develop the levers of deterrence available to it as a nation state to increase the costs for adversaries who target Australian citizens and businesses. An example of this is participating in and leading coordinated disruption operations with international and private sector partners.

Australia should expand its use of cyber diplomacy including investing in regional capacity building, leading multilateral initiatives to promote norms of responsible state behaviour, and embedding cyber themes into broader trade and security agreements. Government should continue to invest in coordinated, principle-based cyber diplomacy that incurs consequences for malicious actors. By combining attribution, advisories, sanctions, and broader cyber diplomacy, Australia can help create a global environment where malicious cyber activity is harder to conduct and easier to discourage.

47. Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?

Australia should strengthen its role as a digital partner to Southeast Asia and the Pacific, combining policy engagement, aid programs, and digital diplomacy to support the adoption of strong, resilient cyber policies across the Indo-Pacific.

A key priority should be promoting secure cross-border data policies as the foundation for a unified approach to cybersecurity. Trusted data flows across the region ensures that emerging technologies and cutting-edge cybersecurity capabilities remain accessible to all countries, regardless of size or resources. This enhances regional

security and drives regional growth by ensuring Indo-Pacific nations can fully participate in the global digital economy.

Australia should use regional forums such as ASEAN, APEC, and the Pacific Islands Forum to advance this agenda. These platforms provide opportunities to coordinate policy, share best practices, and encourage the adoption of international standards across diverse economies.

49. *In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?*

50. W*hat regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment?*

By championing alignment with international standards, enabling secure cross-border data flows, and embedding modern cyber practices in global frameworks, Australia can shape Horizon 2 to advance both its national interests and its standing as a leader in the global digital economy.

Australia should focus its efforts on international forums and standards bodies that drive practical cybersecurity outcomes and promote interoperability. Key venues include the International Telecommunication Union (ITU), the International Organization for Standardization (ISO), and regional forums such as ASEAN and APEC. ISO standards, including the ISO 27000 series and frameworks for security operations centres (SOCs), provide a strong baseline for international regulatory alignment.

A priority area for international alignment is the simplification and harmonisation of government security certifications for the use of cloud-based services. Currently, certification regimes across the region are highly fractured, creating unnecessary barriers for procurement and slowing the adoption of secure cloud technologies by

governments. Alignment would deliver strong productivity gains for governments and lower the barrier for Australian companies selling to regional governments across the region. It does this by streamlining procurement, lowering costs by reducing compliance duplication, and enabling faster access to modern, highly-secure solutions.

Fragmented or localised data requirements undercut the effectiveness of both government and private sector defenders. Regulatory frameworks should prioritise clear and harmonised requirements on incident reporting timelines, cyber threat intelligence sharing, and the use of modern cybersecurity approaches such as cloud-based EDR. Above all, Australia should reinforce support for global cross-border data flows for cybersecurity purposes to better combat global adversaries.

In addition, preservation of the global domain name system and open protocols is fundamentally important to enable cybersecurity visibility, detect cyber threat actors, and mitigate exposed risks; and ensure the ongoing interoperability of the Internet. For example, cybersecurity companies need access to DNS resolution data to identify spoofed addresses and the bad actors behind them. It is also security best practice for companies or Managed Service Providers to proactively review communications with their servers and IP addresses to see if an external website is inadvertently exposed.

VIII. CONCLUSION

The Australian Department of Home Affairs discussion paper provides a thoughtful analysis of a complex legal and policy area. As updates to Australia's National Cyber Security Strategy move forward, we recommend continued engagement with stakeholders.

Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any legislative updates and proposed rulemaking focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

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

Drew Bagley CIPP/E Brian Fletcher

VP & Counsel, Privacy and Cyber Policy Director, Public Policy APJ Email:

policy@crowdstrike.com

III. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms 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/.