29 August 2025
Department of Home Affairs
Submitted online via webform at homeaffairs.gov.au

Cisco submission to 'Charting new horizons: developing horizon 2 of the 2023-2030 Australian cyber security strategy' policy discussion paper

Cisco welcomes the opportunity to provide a submission to the 'Charting new horizons: developing horizon 2 of the 2023-2030 Australian cyber security strategy' policy discussion paper.

This submission is made with contributions from across the company, including our legal, government affairs, security and trust office, engineering and from the expert cyber security team at Splunk - a Cisco company.

We wish to commend the Australian Government for the ongoing and open commitment to engaging with industry and the wider community on the future elements of the 2023-2030 cyber security strategy.

Cisco recognises the significant success the government has made in implementing Horizon 1 of the strategy, including the passage of Australia's first Cyber Security Act, the continued evolution of the Security of Critical Infrastructure (SOCI) framework and the recent 2025 updates to the Protective Security Policy Framework (PSPF). These foundational initiatives reflect a strong commitment to uplifting Australia's cyber resilience and national security posture.

We hope that our submission provides the government with ideas and information that will guide the Horizon 2 development. Together, Cisco and Splunk are ready to assist the government to scale cyber maturity across the whole economy and help foster a culture of productive and secure digital transformation in the era of AI and quantum computing.

We would welcome the opportunity to expand on our submission. Please contact our Director of Government Affairs for Australia, [redacted], at [redacted] or [redacted] for further comment or information.

Cisco Systems Australia Pty Ltd
[redacted]

Cisco submission to 'Charting new horizons: developing horizon 2 of the 2023-2030 Australian cyber security strategy' policy discussion paper

Cisco welcomes the opportunity to provide a submission to the 'Charting new horizons: developing horizon 2 of the 2023-2030 Australian cyber security strategy' policy discussion paper.

We also congratulate the government and the team at the Department of Home Affairs for their ongoing engagement with industry and the wider community on this crucial policy issue. This practice has helped drive the success of Horizon 1 of the *Australian cyber security strategy 2023-2030*, as evidenced by Australia's rise in the rankings of the National Cyber Security Strategy Index from 40th in 2023 to 11th in 2025.[1]

This submission is made with contributions from across Cisco, including our government affairs, security and trust office, engineering and the expert cyber security team at Splunk – a Cisco company.

The three-part approach to the discussion paper is welcome with part 1 providing an update on the implementation of Horizon 1, part 2 framing the potential areas of focus for Horizon 2 and the proposed evaluation methodology, and part 3 a shield-by-shield view of Horizon 2 with discussion questions.

In the following detailed comments, Cisco has addressed the relevant questions in part 3 and excluded those that we have not responded to. We have also provided some general observations throughout.

2. Developing our vision for Horizon 2

2.1 Outlook for Horizon 2

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?**

Within the timeframe of the *2023-2030 Australian National Cybersecurity Strategy*, two technology developments that already have significant cybersecurity implications, are generative AI and quantum computing.

Artificial Intelligence (AI)

Based on Cisco's research and our practical deployment of AI infrastructure and services, there is a dual imperative around AI – leveraging AI to enhance and strengthen cybersecurity defences and ensuring the inherent security of AI systems themselves.

AI for enhanced and strengthened cybersecurity

1. **AI is expanding and reshaping the threat landscape**

Adversaries are actively incorporating AI to enhance the speed, scale and sophistication of their operations. Generative AI is being used to automate and personalise phishing attacks, generate malicious code, and even mimic trusted communications, thereby

[1] National cyber security index - https://ncsi.ega.ee/country/au/

lowering the barrier to entry for cybercriminals and increasing the effectiveness of social engineering campaigns. At the same time, the widespread deployment of AI technologies – particularly large language models – has significantly expanded the attack surface. Organisations are increasingly integrating AI into their environments without fully understanding and addressing the downstream security implications, including model poisoning, data leakage and API abuse.

2. AI is transforming cyber defence

While AI introduces new risks, it also presents powerful opportunities to enhance cyber resilience. The evolving threat landscape, characterised by increasingly sophisticated cyberattacks, necessitates a shift in how organisations approach cybersecurity. AI offers a powerful capability to address these challenges by improving threat detection, prediction and response through:

1. Proactive defence: AI can rapidly analyse vast amounts of data, enabling the identification of anomalies that signal cyberattacks or malicious code. This moves cybersecurity from reactive remediation to proactive prediction and prevention, allowing organisations to strengthen their posture before attacks occur, and
2. Automated response: AI can significantly reduce incident response times and tailor security policies to specific organisational needs, augmenting human insight and enabling security teams to operate at machine speed.

Cisco and Splunk are leveraging AI and machine learning to accelerate anomaly detection, streamline investigation workflows and reduce alert fatigue across security operations. Publicly available data from Splunk's State of Security 2025 report indicates that 59% of organizations surveyed have moderately or significantly boosted their efficiency with AI.2 These improvements are essential to managing modern threats at scale, and the government should play a role in encouraging the safe and responsible adoption of AI in cyber defence.

3. AI will reshape workforce requirements

While the discussion paper acknowledges the current shortage in cyber security professionals, we urge the government to also consider the evolving nature of cyber work in an AI-enabled world. AI has the potential to augment cyber professionals by automating routine tasks, enhancing productivity and enabling smaller teams to manage more complex environments. This could, over time, shift the workforce challenge from raw numbers to ensuring the right mix of skills—particularly in areas such as AI model evaluation, adversarial testing and ethical deployment. The emphasis should be not only on volume, but also on the type, skillset and adaptability of the workforce.

As an example, GenAI can modernise cybersecurity operations by enhancing system usability and democratising access to advanced security tools. For instance, Cisco's AI Assistant for Firewall[1] allows configuration with natural language, lowering the barrier to entry for non-experts and improving the efficiency of Security Operations Centers (SOCs). We are now entering an era where computers will speak our language instead of requiring humans to learn theirs. The ability to interact with sophisticated security technology in English can help address the global shortage of cybersecurity professionals by making complex tasks more accessible. We will bridge the gap between certifications, training and real-world experience to tap currently under-utilised pools of talent and creativity.

Cisco's internal experience developing and deploying SOC AI CoAnalysts, utilisation of AI/ML models for detections and efficiency outcomes such as playbook metric and analyst comment summarisation has delivered significant benefits including 25% improved time to triage, 64% improved time to contain and 61% improved time to remediate. Splunk's Student-Powered Security Operations Centers (SOCs)[2] offers a vital solution for higher education institutions to combat escalating cyber threats and the shortage of cybersecurity professionals by leveraging student skills for incident response, providing them with invaluable real-world experience and strengthening institutional defences.

4. AI readiness and future procurement planning

Finally, AI infrastructure readiness should be a strategic consideration for both government and industry. Organisations need the capability—not just to adopt AI—but to do so safely, ethically, and at scale. This includes having the bandwidth, data infrastructure, and governance frameworks in place. As public and private sector entities undertake major ICT and hardware procurements, there is a growing need to consider AI compatibility and readiness at the point of purchase. Given the long lifecycle of such investments, failing to do so may result in systems that are outdated or unable to accommodate the secure deployment of AI by the time they are operational.

The Cisco *Cyber security readiness index* provides further details about the state of cyber readiness across the world and in Australia specifically. From the 2024 to 2025 report, readiness remains low globally year over year, as companies underestimate the complexities of AI.[2] Only 4% of organizations reached the 'mature stage' of cybersecurity readiness, up just 1% from the year before.

AI is reshaping the security landscape, adding layers of complexity to threats and the measures needed to defend against them.

This evolving threat landscape, characterised by increasingly sophisticated cyberattacks, necessitates a shift in how organisations approach cybersecurity. AI offers a powerful capability to address these challenges by improving threat detection, prediction, and response.

To effectively grasp the opportunities of AI for enhanced and strengthened cybersecurity, Cisco recommends the following:

1. **Foster standards development:** Australia should partner with industry on the development of risk-based standards for use of AI, to cement the advantages of defenders to predict and prevent harms and respond with the power of machines and the scale of networks when successful exploits are discovered. Additional collaboration in standards bodies will also be necessary around the security of AI

[2] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m05/cybersecurity-readiness-index-2025.html#blade_global-readiness

systems themselves, and should include: model risk assessment; empowering enterprises to select and limit applications based on model security; data loss prevention to avoid unintended disclosure of personal information, trade secrets, and intellectual property; and deployment of effective guardrails to detect and prevent "drift" in model behaviour over time.

2. **Leverage industry-led standards and limit regulations to address serious harms:** Uniform, risk-based, non-regulatory frameworks, preferably based on internationally recognised standards, will foster trust and streamline compliance and strengthen national security. Where regulations are necessary, they should be narrowly scoped to address actual risk of significant harm that are not already effectively captured by existing legal authorities. Requirements should be aligned wherever possible with principles of risk management and to widely adopted internationally recognized standards.

3. **Ensure regulatory alignment:** Divergent and conflicting regulations create complex and costly landscapes that hinder innovation. Even where generally aligned, we also need consensus on thresholds. The difference in mandatory incident reporting for both impact thresholds and time periods across nations and even sectors and legislation within sectors is a significant burden to industry. Any necessary AI security regulations should avoid repeating this outcome. This includes encouraging mutual recognition of certification regimes and avoiding local requirements that differ from internationally recognised standards.

4. **Support trusted technology:** Encourage the adoption of trusted technology in digital networks, including connectivity and cloud infrastructure, while avoiding restrictions based solely on country of origin to maintain supply chain resiliency.

Ensuring the inherent security of AI systems supports innovation

While AI offers immense benefits, its widespread adoption also introduces new vulnerabilities and risks. Ensuring the security of AI models and their underlying infrastructure is paramount to fostering public trust and safeguarding national security.

- **Addressing AI-specific risks:** AI-associated risks such as data leakage, data poisoning, training data extraction, prompt injection and insecure output handling must be proactively addressed. Cisco's State of AI Security Report[3] has documented instances of successful attacks targeting parts of the AI value chain.

- **Real-time protection:** High-performing AI models do not automatically equate to highly secure models. Developers and deployers need a comprehensive understanding of potential weaknesses. Solutions like Cisco AI Defence[4] provide robust tools for continuous detection and protection against emerging threats in AI applications, including data loss prevention and "drift" in model behaviour over time.

---

[3] https://www.cisco.com/c/en/us/products/security/state-of-ai-security.html
[4] https://www.cisco.com/site/us/en/products/security/ai-defense/index.html#tabs-9da71fbd27-item-1288c79d71-tab

- **Supply chain security:** Organisations must understand the potential risks and vulnerabilities associated with third-party software, AI models and data within the AI supply chain. Threat actors can introduce corrupted data into training datasets or inject malicious code into open-source AI repositories. New AI-powered tools can foster our ability to assess and manage risk at speed and scale.

We recommend that Australia consider the following approach:

1. **Risk management frameworks:** Ensure that agencies deploying AI define clear risk measurement and mitigation strategies, aided by established frameworks such as the U.S. National Institute of Standards and Technology (NIST) AI Risk Management Framework (RMF).
2. **Collaborate on testing and validation:** Work with private sector partners to support pre-and post-deployment testing of AI models, encouraging automated red teaming and the validation of AI systems both prior to initial use and over time to address risk of "drift."
3. **Mitigate supply chain risks:** Collaborate with stakeholders to evaluate weaknesses in publicly available AI models and promote market-based solutions to address these risks within the AI supply chain.
4. **Promote trusted vendors:** Encourage technology replacement policies and behaviours to avoid potential security risks associated with underlying digital networks that may contain untrusted vendor technology. Ensuring that foundational technology stacks are designed, developed and deployed by trusted and trustworthy partners is essential given the dependence that such systems will have on cloud-based management and continuous deployments of code updates and feature upgrades.
5. **Participate in standards development:** Support participation in global AI standards discussions to facilitate market access and reduce duplicative compliance obligations for businesses, emphasising alignment with internationally recognised standards in AI security.

Quantum Computing

Quantum computing will fundamentally reshape the cyber security outlook. Quantum capabilities are expected to break traditional encryption methods, potentially within the timeframes associated with Horizon 2. While the government has rightly focused on enhancing quantum readiness – including the implications for legacy encryption – there remains a critical need to extend this focus to state and territory governments, as well as to critical infrastructure.

A proactive step would be to require all Security of Critical Infrastructure (SOCI) regulated entities to consider their post-quantum cryptography (PQC) readiness as part of existing risk management obligations. This approach would not only raise awareness of the issue but also embed quantum strategy planning into board-level decision-making, ensuring that leadership is actively considering the long-term resilience of their organizations against the risks posed by quantum advances.

Advances in quantum computing and the capability to break some of the widely used encryption algorithms relied on globally by governments, businesses and citizens are rapidly approaching. The need to start the planning process to move to Quantum Resistant (QR) algorithms and PQC is now. While dates for completing migration to PQC algorithms vary across peer nations such as Australia, the UK and the US – around 2030-2035 depending on the exact use case – conducting a cryptographic "stocktake" is a common recommendation for the initially planning.[5] Additionally, we are entering the window of technology refresh lifecycle where the products procured today will need to be PQC capable before their end of life. The Australian Signals Directorate in both guidance and the Information Security Manual (ISM) highlights the need to consider PQC roadmaps in technology procurement. However, to prepare the whole of the Australian economy, alternate awareness and policy interventions may be required.

A "PQC-driven" technology refresh also presents the opportunity to address the LDOS (Last Day of Support)[6] issue causing widespread exposure to unpatched security vulnerabilities and help remove some roadblocks for IPv6 support that persist in Australia[7].

We recommend that Australia consider the following approach:

1. Raise PQC as a threat under the SOCI Cyber Hazard that should be acknowledged and addressed under the RMP process
2. The CISC conduct awareness sessions and risk advisory notes on PQC for the CI audience.

2.3 Monitoring progress in a changing world – a conceptual framework for evaluating cyber security outcomes

3. **Does the high-level Model resonate and do you have any suggestions for its refinement?**

Conceptually, the proposed linking of interventions to (measured) outcomes is valid, however it is important to ensure that quality and quantity are being measured and evaluated against progress toward attaining the goal. One of the challenges to measuring progress is visibility – the intervention may be government designed or administered, yet some outcomes will be at the organisation level, often within the private sector. Organisationally, there are operational cyber security measures and metrics such as NIST SP 800-55: Measurement Guide for Information Security, Cisco internally developed Unified Security Metrics (USM) for security posture measurement[8], or guidance from Splunk on SOC Metrics[9].

[5] https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/planning-post-quantum-cryptography
[6] https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-update-your-device-and-software/end-support
[7] https://blog.apnic.net/2024/11/21/just-how-widely-adopted-is-ipv6-in-australia
[8] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/unified-security-metrics-framework.pdf
[9] https://www.splunk.com/en_us/blog/learn/security-operations-metrics.html

If the ultimate outcome is cyber resilience, then the measures and metrics need to reflect the full spectrum of what is cyber resilience – at a high level to anticipate, withstand, recover and evolve.

4. Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?

Cisco welcomes the partnership approach proposed with industry, academia, data agencies, and the community in the design of metrics and measurements for the strategy outcomes. It is critical that metric design is done as part of intervention design with buy-in from all parties such that the method and means of sharing metrics of outcomes results from outside of government back into the department is already agreed from the outset.

3. Shield-level focus for Horizon 2

3.1 Shield 1: Strong businesses and citizens

5. What could government to do better target and consolidate its cyber awareness message?
6. What programs or pilots have been successful in this context? What additional supports could be developed or scaled-up to address these issues in partnership with both education stakeholders and those with technical cyber security expertise?

The government's approach to engaging with industry partners who are willing to help support the policy objectives in the 2023-2030 cyber security strategy is a powerful way to help deliver effective and efficient cyber security messaging to the wider community.

Home Affairs should consider convening a Ministerial, then Department-led working group of industry, community and academic participants to focus exclusively on achieving a specific goal in relation to cyber awareness which can be measured and tracked. All participants can bring resourcing, ideas and a commitment to achieve an agreed goal that ties in with Australia's broader productivity, economic growth and community safety agenda.

An example of the power of a government-auspiced and industry/community/academia driven group like that suggested above is the group that delivered 'national teleworking week' and associated activities in 2012, to help drive an increase in remote, home-based or hub-based work practices in line with one of the goals in the Australian government's National Digital Economy Strategy.[10]

To give effect to the goal of 'doubling the number of teleworkers in the Australian economy', the Minister for Communications convened a meeting with industry, community and academic participants then directed the Deputy Secretary of the Department of Communications (Abul Rizvi) to lead a working group to come up with ideas about how to achieve this policy goal. The outcome was a range of initiatives that culminated in

[10] https://apo.org.au/node/227751#:~:text=online%20participation%20by%20Australian%20households,leading%20digital%20economy%20by%202020.

‘national teleworking week’ with an opening conference at the University of Melbourne that was launched by the Prime Minister (Julia Gillard), Minister’s for Communications (Senator Stephen Conroy) and Employment and Workplace Relations (Bill Shorten), the United States Ambassador to Australia, and many others. The industry participants drove this and many other initiatives, guided by the government’s policy initiative and high-level executive support.

Working from home or remotely is now a widely established practice across every industry sector, facilitated by Australia’s high penetration of high-speed broadband. While there are a range of reasons for the success of that policy, bringing industry and other participants together to achieve a shared policy outcome is an excellent model that could be followed to achieve greater education and understanding of cyber security across Australia.

7. **How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?**

Below, we make some comments about our partnership with InfoXchange. Having NFP representation on the Executive Cyber Council would be helpful as they are currently not represented.

8. **How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience?**

The Australian banking sector is a good example of where cyber security education and awareness has been embedded into an existing business relationship between industry and SMEs. National Australia Bank (NAB) has also partnered with security industry partners to provide cyber security offers and discounts to their customers through their Business Security Hub[11]. Cisco has partnered with NAB and OutcomeX to offer protective DNS security with Cisco Umbrella[12]with the purpose of uplifting SMB cyber security.

In addition to general cyber security awareness outreach programs from the government, opportunities to promote cyber security uptake through existing business interactions such as the banking example should be explored.

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?**

Cisco welcomes the government’s specific focus on the NFP sector where cyber security uplift is crucial. We have worked with many NFPs to help improve their cyber security posture, from providing technical advice, assistance and equipment and services, to knowledge sharing and education of their staff. In addition, Cisco’s employee volunteering program has seen many hours of Cisco professional support provided to help NFPs

[11] https://www.nab.com.au/about-us/security/online-safety-tips-business
[12] https://www.nab.com.au/about-us/security/online-safety-tips-business/cyber-threats-business-protection

deploy and configure technologies to help improve overall cyber hygiene and data resilience.

NFPs often face challenges that other businesses and organisations may not. For example, depending on the sector, some NFPs may be high risk targets for cyber disruption or data breaches due to the nature of the services they provide their members. Cisco has long been a member of the Diversity Council of Australia (DCA) (and participated at the board level) and the DCA has been subject to malicious campaigns directed at the organisation in response to its research on diversity and inclusion issues. In addition, NFPs often hold personal and financial information of their clients and members and can sometimes find it difficult to fully resource their cyber security capabilities when balancing the need to service their clients.

Cisco partners with InfoXchange, a not-for-profit social enterprise that has been delivering technology for social justice for 35 years. With over 140 staff across Australia and New Zealand, InfoXchange tackles the biggest social challenges through the smart and creative use of technology.

In their most recent report, *Digital Technology in the Not-for-Profit Sector; 2024,* InfoXchange outlines a range of reasons about why the NFP sector is inherently vulnerable to cyber attacks, such as the lack of funding to invest in cyber security, reduced focus on cyber safety plans, the use of volunteers and more. Innovative technologies such as AI and digital data collection present additional challenges and concerns, but they also offer the potential for greater efficiencies and impact if integration can be managed well.

InfoXchange's report outlines that cyber security remains a key challenge for the sector – 57% of responding organisations do not have multi-factor authentication (MFA) for all Internet-facing information systems holding sensitive information. This is a critical concern, but it is an improvement from last year, when 62% reported not having MFA turned on for all Internet-facing information systems. Only 20% of organisations reported conducting regular cyber security awareness training for staff and volunteers on security-related threats and risks. This is up 8% from last year, but there is significant room for improvement, with a myriad of resources available for cyber security education. Only one in 5 organisations have a plan to improve their cyber security protections.[13]

This information suggests that the NFP sector would benefit greatly from government support through increased funding specifically targeting cyber security uplift across the NFP sector.

A further government initiative could be to bring together a Ministerial round table including the leaders of technology companies that provide discounted products and services, as well as no-cost education and volunteering programs with leaders from the NFP sector. This round table could provide ideas for the government to consider and could mimic the government's economic round table with a focus on improving the productivity of the NFP sector.

---

[13] https://www.infoxchange.org/au/digital-technology-not-for-profit-sector

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?

A trend observed by Cisco Talos is that ransomware actors overwhelmingly leveraged valid accounts for initial access in 2024[14], with this tactic appearing in almost 70% of related cases. While exploitation of Internet-facing applications and other techniques is still common, this tactic is facilitated in large part by the sale of compromised credentials on dark web forums.

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

Given the trend observed by Cisco Talos, efforts to better secure credentials such as MFA adoption, strong unique passphrases, passwordless solutions and secure digital identities should continue to be promoted and highlighted. Horizon 1 initiatives to disrupt the entire ransomware ecosystem need to continue, including efforts to disrupt Initial Access Brokers.

14. Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector? If so, what were the vulnerabilities and impacts that your community faced?

Addressing end-of-life (EOL) equipment is a strategic imperative for enhancing cybersecurity resilience, particularly as the pace of digital transformation accelerates and the threat landscape grows increasingly complex. EOL systems, once no longer supported by vendors, cease to receive vital security updates and patches. As a result, any vulnerabilities discovered in these systems remain unaddressed, creating exploitable entry points for malicious actors. The continued presence of such obsolete technology within critical systems not only increases operational risk but also contributes to mounting technical debt, diverting resources toward maintaining legacy infrastructure rather than enabling modernisation.

The risks associated with EOL technology are particularly pronounced in critical infrastructure sectors, including finance, energy, water, and healthcare. The operational continuity of these sectors is fundamental to national security, economic stability, and public welfare. A successful cyberattack in these domains can trigger immediate and widespread disruptions, with the potential for cascading effects across interconnected industries.

Despite the severity of these risks, existing funding structures and procurement approaches have unintentionally fostered an environment where technical debt is perpetuated. Investment is frequently directed toward sustaining outdated systems rather than prioritising their remediation or replacement. This dynamic not only constrains innovation and limits the adoption of enhanced security practices but also leaves critical infrastructure increasingly exposed to preventable threats. A significant proportion of

[14] https://blog.talosintelligence.com/year-in-review-ransomware

cyber incidents today arise from the exploitation of known, but unpatched, vulnerabilities—often present in obsolete systems.

A more proactive and systematic approach to managing EOL technology is required to address these challenges effectively. This includes the establishment of robust asset management practices, the adoption of lifecycle management policies that mandate timely replacement or mitigation of legacy systems and the alignment of funding models to support remediation efforts. Moreover, enhanced transparency, clear regulatory guidance, and sector-wide information sharing should be promoted to facilitate early identification and management of emerging risks. By prioritizing the mitigation of EOL equipment vulnerabilities, policymakers and infrastructure operators can significantly bolster the resilience of critical sectors, reduce systemic cyber risk and better safeguard the essential services that underpin economic and societal well-being.

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

While still relatively early in its execution phase, the Australian Government's *Security of Critical Infrastructure Act* has been an important regulation across all Australian critical infrastructure sectors. The principles-based approach and focus on risk management is driving an anecdotal uplift in security awareness we see from Cisco customers when they procure both on-premise products but especially cloud services. The reforms to the Privacy Act 1988 have also acted to help reduce cyber risk in Australia.

3.2 Shield 2: Safe technology

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?

ASD and international partners have produced guidance not only to consumers but also manufacturers of edge devices.[15] While secure-by-design and secure-by-default adoption are important for vendors, equally important is lifecycle management of these devices – secure configuration, patching and end of life management. In 2025, we still observe abuse of vulnerabilities dating back many years across Cisco and other network and security infrastructure vendors[16]. Looking to the future however, cloud-service delivery models either make patching a responsibility of the cloud service provider or, at minimum, create awareness and improved patch application processes when administered from the cloud. Cloud-delivered and software-defined solutions also typically rely on configuration templates and patterns, providing an easier means to apply mitigations where patching is not immediately available.

[15] https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/network-hardening/securing-edge-devices/security-considerations-edge-devices

[16] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2

While the security of cloud services is paramount, we should not lose sight that for some organisations, security risks are also reduced by the adoption of cloud service delivery models.

19. How should the government work with you to support consumers and end-users to be more informed about cyber security in their products and protect themselves from cyber threats?

The Horizon 1 initiative – Labelling Scheme for Smart Devices has only recently commenced. The outcome of this initiative is important for informing further initiatives for consumer awareness.

21. How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors?

To enable this conversation, it would be helpful to have an early release or potential model for the Voluntary Data Classification Framework[17] as a reference point. It would be helpful to have a baseline to provide a degree of consistency, even in a simplified form, for these discussions.

23. What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies?

The government should encourage organisations to adopt a culture of undertaking impact assessments. For example, whether as a developer or consumer, Cisco conducts Privacy Impact Assessments and AI Impact Assessments as a requirement of our corporate governance processes[18]. The impact assessment not only looks at the safe and secure use of new technologies from a business perspective, but also alignment with Cisco Responsible AI Principles[19], human rights, environmental, and other commitments[20]. This governance can be agnostic to any specific technology development.

3.3 Shield 3: World-class threat sharing and blocking

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?

25. Does the government need to provide clarity on permissible and non-permissible Active Cyber Defense in the Australian Context?

Where governments consider taking more assertive actions on cyber defense, the types of permissible offensive actions should be clearly defined and limited, with consultations, oversight and accountability, and due care given to anticipated and unintended

[17] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/technology-and-data-security/voluntary-data-classification-framework
[18] https://www.cisco.com/site/us/en/solutions/artificial-intelligence/responsible-ai/index.html
[19] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-responsible-artificial-intelligence-principles.pdf
[20] https://www.cisco.com/c/m/en_us/about/csr/esg-hub.html

consequential damage. Where such government-led actions involve the private sector, a careful balance needs to be struck between governments taking steps in an active way that enters private spaces beyond their own network boundaries and ensure legal liability protection is adequately and appropriately addressed where private sector entities are involved. The policy should not engender actions that become irresponsible or create a market for cyber mercenaries. Implementing an approach such as a Vulnerabilities Equity Process[21] to help vendors find and fix vulnerabilities found while taking actions would help balance the public interest and protect critical infrastructure. Governments should also not impose mandates on vendors that could break security mechanisms (such as encryption) or create backdoors or other measures that would weaken the security posture of products and services.

Australia faces an increasingly complex and hostile cyber threat environment, with state-based actors and criminal syndicates leveraging automation, AI, and globally distributed infrastructure to conduct malicious operations at scale. In response, the Australian Government has rightly invested in sovereign capabilities across the full cyber spectrum—from the public acknowledgement of offensive cyber operations at one end, to the strengthening of defensive and reactive measures at the other. This includes the evolution of the SOCI framework, deeper collaboration with critical infrastructure sectors, and the promotion of baseline cyber hygiene controls such as the Essential Eight.

However, there remains a significant opportunity to strengthen collaboration more closely with trusted private sector technology and cyber security companies to proactively detect, disrupt, and prevent cyber adversaries *before* they can impact Australian systems, services, and citizens. This middle space does not require new regulations, but rather deliberate, structured partnerships with key technology and infrastructure providers.

Many of these providers - across telecommunications, cloud services providers, networking and cyber security companies - have frontline visibility into malicious activity, often seeing emerging threats before they are widely known. They are often able to block or disrupt threats in real time for thousands of customers simultaneously. Some entities may even possess the ability to remove malicious infrastructure or actors from their platforms as part of their terms of service — rapidly neutralizing adversary infrastructure and capabilities. Harnessing these capabilities through stronger public-private partnerships can materially enhance Australia's collective cyber resilience and adversary disruption efforts.

Australia may wish to explore a targeted disruption proof of concept in collaboration with a select group of trusted technology and cyber security partners. We recommend the Government consider initiating such a pilot to test and refine coordinated operational responses to malicious cyber activity, leveraging the unique visibility and capabilities of industry to detect and disrupt our cyber adversaries at scale.

26. How could government further support industry to block threats at scale?

Australia's cyber threat environment is evolving at a pace and scale that traditional, organisation-by-organisation defences cannot match. Attacks are increasingly

[21] https://www.ncsc.gov.uk/blog-post/equities-process

automated, global in reach, and designed to exploit the foundational layers of our digital ecosystem. This makes it clear that a whole-of-ecosystem "threat blocking at scale" strategy—often referred to as "clean pipes"—is now essential to protect the everyday citizen.

Telstra has already demonstrated leadership through its Clean Pipes initiative, which applies DNS filtering to block access to known malicious domains. While an important first step, DNS filtering is only part of the solution. Adversaries are exploiting multiple parts of the ecosystem—communications service providers (CSPs), Internet service providers (ISPs), web browsers, domain registrars, cloud platforms and more. A truly national approach must therefore be broader, coordinated and embedded across all layers of the ecosystem. A threat blocking approach recognises that many attacks can be stopped before they reach millions of Australians, rather than relying solely on fragmented, individual defences.

31. How could government better incentivise businesses to adopt vulnerability disclosure policies?

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

Australia should not establish a separate, national vulnerability disclosure program. Creating a standalone scheme would add unnecessary complexity for technology providers – particularly multinational companies – that already operate global vulnerability disclosure and coordinated reporting processes. These firms rely on consistent, streamlined mechanisms to triage, remediate and communicate risks quickly across jurisdictions. Fragmenting disclosure obligations risks duplicating effort, confusing researchers, and slowing remediation timelines.

3.4 Shield 4: Protected critical infrastructure

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 was a needed piece of Australian legislation to raise awareness and drive action across the diverse set of CI sectors. Whilst some sectors had historical maturity in treating the hazards covered under the SOCI RMP process, many did not. We commend that the legislation is principles-based and remains so through subsequent amendments. Key to the understanding of obligations has been the publications and outreach activities of the Critical Infrastructure Security Sector. Given SOCI is still *relatively* new, we recommend a period of stability against ongoing changes and the consideration of how the proposed monitoring and measure of outcomes could be applied. We also suggest a period of change freeze for SOCI for the legislation and framework itself. The obligations should stay current and adapt to emerging threats, such as adversarial AI and quantum computing challenges to cryptography.

34. Are there significant cyber security risks that are not adequately addressed under the current framework?

The framework requires that risks are identified and managed. Where greater attention could be focused is on raising awareness of new risks. Specific examples of technology risks raised in this submission include AI where the CISC have recently published an AI in Critical Infrastructure Factsheet.[22] As highlighted, Post Quantum Cryptography is an area where the CISC could raise awareness under the existing framework.

35. **Is the regulatory burden on industry proportionate to the risk and outcomes being sought?**

36. **What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices?**

37. **What role should government play in enabling uplift, including through tools, guidance or incentives?**

To date, much of the policy emphasis has been on threats and baseline controls – such as ISO 27001 and the Essential Eight – but comparatively little attention has been directed towards the modernisation of the Security Operations Centre (SOC). The SOC is the nerve centre for detecting and mitigating cyber threats in near real time. Without modernisation, organisations risk falling behind adversaries who are increasingly automating and accelerating their attacks. A modern SOC should not only leverage automation and AI but also be measured against key operational metrics such as Mean Time to Detect (MTTD) and Mean Time to Triage (MTTT). Embedding these requirements into regulatory and policy frameworks would drive greater accountability, enhance visibility, and ensure that organisations are continually improving their defensive posture.

There is also a need to invest in and establish SOC capabilities across federal, state and territory governments as some agencies lack SOC capabilities altogether, limiting their capacity to centrally detect, analyse and mitigate threats across their environments. Addressing this gap is essential to achieving whole-of-nation resilience. Implementing the key controls such as patching and logging is made substantially more difficult without a SOC. By strengthening SOC capabilities across both public and private sectors, the government can help lift national resilience against sophisticated cyber threats.

To ensure the continuity and reliability of essential services, the government should also emphasise the importance of observability capabilities across all Systems of Government Significance and Systems of National Significance. Observability should be elevated in policy, guidance and resilience discussions as a foundational requirement – just as vital as patching and access management – because without it, threats and application issues can remain hidden until they cause major disruptions or outages. Unlike traditional monitoring, observability delivers real-time, end-to-end visibility into the health and performance of digital environments. This capability enables agencies to detect anomalies early, anticipate system failures and respond to issues before they escalate into service outages. As governments and critical infrastructure increasingly relies on AI tools and digital platforms to deliver frontline services, observability is no longer optional – it is fundamental to operational resilience. A failure in these systems risks not only disrupting essential services but also eroding public confidence in government and the

[22] https://www.cisc.gov.au/resources-subsite/Documents/artificial-intelligence-factsheet.pdf

economy. By embedding observability requirements into agency operations, governments can reduce downtime, detect and prevent fraud and safeguard the continuity of critical services, ensuring they are available to citizens when needed most.

To further improve critical infrastructure protections, we would also encourage the federal government to consider:

1) **Establishing sustained and transparent cyber security investment**: at the federal level, cyber security expenditures are not separately identified, obscuring the level of cyber security investment and making it difficult to measure progress or hold agencies accountable. To continue to build digital resilience, the government should move to a sustained, transparent investment in cyber security. This could include the creation of a clearly defined cyber security budget line that is reported consistently across agencies. Such an approach would strengthen benchmarking and accountability while ensuring that government systems are modernised, resilient and adaptive to an evolving threat landscape, and
2) **Practicing and encouraging simplification and consolidation of cyber security platforms**: fragmented cyber security tools can increase cost, complexity and create talent strain, while leaving critical blind spots in cyber defence. By consolidating and simplifying cyber capabilities into integrated platforms, agencies can achieve end-to-end visibility, streamline operations and harness automation at scale. This approach would not only improve security outcomes but also reduce operating costs and duplication across agencies, freeing resources to be reinvested into resilience and innovation.

38. How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?

That SOCI recognises multiple frameworks including AS/ISO27001, SOC2, AESCSF, NIST CSF is reflected in the types of supply chain security and cyber security assessment questions Cisco receives from customers. We observe that the principles-based approach of SOCI is being adopted by Cisco critical infrastructure customers, but the framework chosen varies by individual organisations.

3.5 Shield 5: Sovereign capabilities

39. What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?

Cisco recommends that the government give deeper attention to the role of AI in shaping Australia's future workforce and sovereign capabilities. As AI becomes embedded across government and industry, it will transform skills demand in profound ways. Studies consistently predict that traditional roles – such as software development – will decline as coding and testing tasks are increasingly automated. At the same time, new demand will surge for skills in AI governance, adversarial AI defence, cyber security, data integrity, and ethical AI design.

To remain competitive and resilient, any national cyber workforce strategy must anticipate these shifts rather than react to them. Training pipelines, university curricula and mid-career transition programs should be explicitly designed to align with AI-driven changes in the labour market. Without this forward-looking approach, Australia risks investing heavily in capabilities that will be redundant within a decade, leaving critical gaps in the very areas that will matter most for national security and resilience.

In addition, the government should deepen structured collaboration between industry, academia, and think tanks to set research priorities and drive innovation in cyber security. Successful models already exist – such as the Cisco National Industry Innovation Network (NIIN), one of Australia's largest innovation networks, which links universities and industry to accelerate digital innovation and build cyber capabilities for government and critical infrastructure. Rather than creating new mechanisms, government could leverage and expand such proven platforms to address joint research needs, reduce duplication, and fast-track outcomes that align with Australia's strategic, economic, and community interests. We refer you to the NIIN's own submission for further details.

To strengthen these efforts, the government should also invest in people-to-people links with academia, including joint research programs, staff secondments, and co-designed policy development activities. This would ensure that policy and practice evolve in tandem, grounded in evidence, innovation and shared capability building.

40. What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM-fields more broadly?

Since 1997, the Cisco Networking Academy – netacad.com – has been operating as a skills-to-jobs program shaping the future workforce, across Australia and around the world. [23]

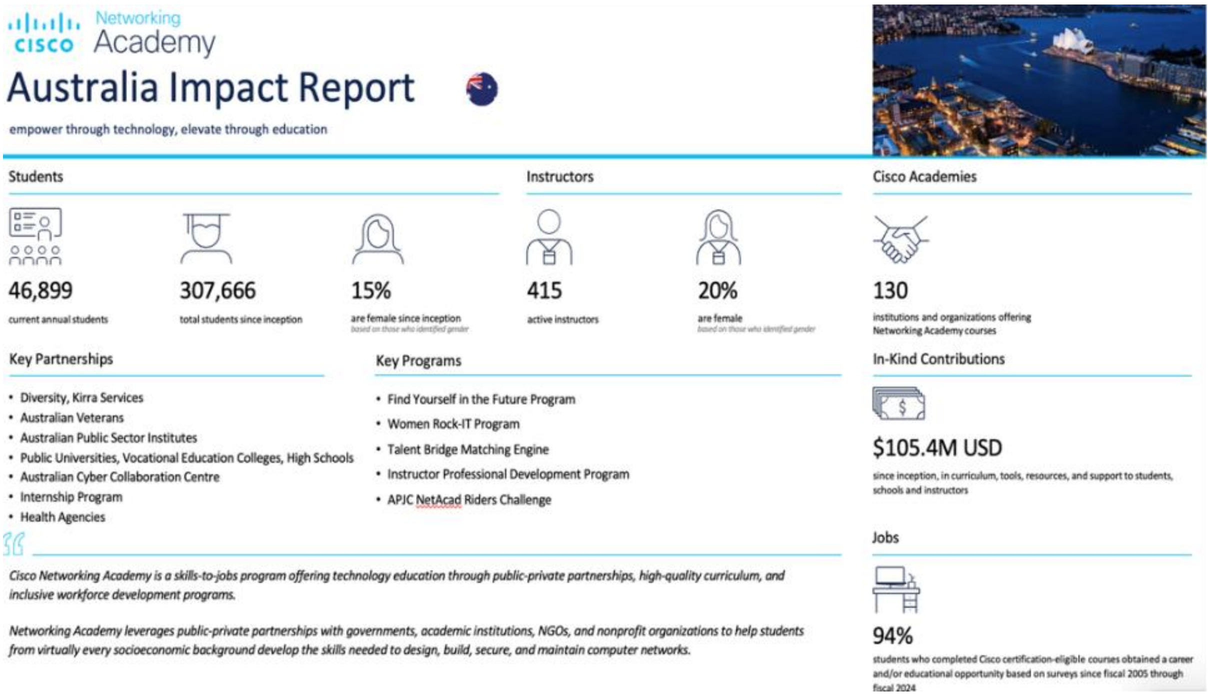
Guided by Cisco's purpose to power an inclusive future for all, this program prepares learners with real-world skills and helps them discover opportunities to apply them. We do this with our progressive education technology platform, leading-edge curriculum, superior learning experiences, and an unparalleled partner ecosystem which have led to us impacting 24 million learners in 191 countries.

Today, in addition to the millions of learners who take our self-paced courses, 31,300 educators deliver our curriculum across 12,100 organizations. 96% of learners who complete our courses find employment or access new educational opportunities. And our ever-expanding ecosystem of partners ranges from the White House and the United Nations to many nonprofits.

From artificial intelligence and sustainability to industry-leading cybersecurity courses taken by millions, we continuously evolve and expand our course catalog so our learners can build the practical skills and deep knowledge they need to harness new technologies and equitably participate in a rapidly changing global economy.

[23] Cisco Networking Academy https://www.netacad.com/

The following infographic provides details about the current Cisco Networking Academy program across Australia.



That this education program has been operating for over 25 years, that it educates people around the world, that it is an example of a long-term public-private partnership between industry and not for profit education providers is evidence of its success.

Other technology industry players have education and skills programs and there is a role for government to provide a pathway and promote access to these programs, which often contain free, self-paced and online courses.

42. **How can industry, academia, think tanks and government best work together to set research priorities and drive innovation to further our strategic, economic and community interests and achieve our common goals?**

Cisco formally established the Cisco National Industry Innovation Network (NIIN) in 2020[24] building upon existing university relationships. The goal of the NIIN in Australia is to create a collaborative platform for industry, academia and government to apply innovation at scale to address significant economic and societal challenges. The outcome has been the establishment of a digital innovation ecosystem that accelerates digital opportunities, fosters industry-led innovation and develops future-ready digital skills through partnerships among universities, companies, and government entities. This collaboration aims to improve Australia's long-term digital economic resilience by solving critical challenges such as climate change, critical infrastructure security, workforce skilling and healthcare delivery.

[24] https://www.cisco.com/c/m/en_au/niin.html

Critical to the success of this model is industry engagement. It is industry that often bring the unique challenges for research and are beneficiaries of the output. To date, the NIIN has over 250 industry projects delivered or in progress[25]. Please refer to the NIIN's separate submission for further details.

3.6 Shield 6: Strong region and global leadership

46. Do you view attributions, advisories and sanctions 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?

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?

Cisco congratulates the Australian government on its work in helping to build capacity and strengthen the cyber security capabilities across the region and especially in the Pacific region.

Cisco was pleased to be able to participate in Pacific Cyber Week (PCW) 2025 and congratulates the Department of Foreign Affairs and Trade and Department of Home Affairs for coordinating a successful week. The presence of so many industry players, academics, distinguished guests and elected and non-elected officials is evidence of the interest in helping to improve cyber resilience and data availability in the region. The government should continue to support PCW and other Pacific capacity building and advocacy activities, such as the Quad and the Cyber and Critical Technology Cooperation Program (CCTCP).

Building local skills and providing education has been a focus of Cisco's involvement in the region. This includes a DNS blocking program in partnership with the University of South Pacific and a commitment to establishing a digital hub to support education and skills uplift – especially cyber security skills – in Fiji and across the Pacific Island nations.[26]

In addition, Cisco has established Networking Academies in Fiji, Tonga, Samoa and PNG as well as in New Zealand. Some 2,900 students are undertaking either accredited Cisco Networking academy courses or self-paced, online pathway courses designed to help find a job in the technology sector. The government could assist this work by again convening industry players to discuss how to better coordinate our efforts in consultation with Pacific Island nation leaders. In a workshop Cisco hosted at PCW, participants from Fiji, Samoa, Tonga and PNG listed skills and education as the barrier they most need to overcome to increase their rate of digital transformation and uplift their cyber security posture. We will be engaging with the leaders of these countries as a follow-up to the PCW workshop and would welcome Home Affairs and DFAT support.

Cisco supports the ongoing work the government is undertaking, through KPMG, to advance the concept of a regional threat blocking capability or shared service. We have

---

[25] https://www.cisco.com/c/m/en_au/niin/projects.html

[26] Cisco and University of South Pacific case study: https://www.cisco.com/site/us/en/about/case-studies-customer-stories/usp.html

highlighted that our partnership with USP is already delivering a service like this to USP students across Pacific Island nations and have offered to share information and provide technical advice to establish a model for how this might work.

The Ambassador for Cyber Affairs and Critical Technology has become a cornerstone of Australia's international engagement on cyber and emerging technology. The role has strengthened Australia's leadership in global cyber diplomacy, built trusted partnerships, shaped international norms and advanced capacity-building across the Indo-Pacific. It has also ensured that critical dialogues on responsible state behaviour, AI, quantum technologies and other emerging risks are embedded within broader foreign policy and national security agendas. Given the accelerating pace of technological change and its security implications, continued support for this role at senior ambassadorial level is essential. Sustaining visible leadership demonstrates Australia's long-term commitment to an open, secure and resilient digital order, while ensuring cyber and technology remain at the forefront of global cooperation and national resilience efforts.

48. **Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope?**

We congratulate the Government on the launch of the Cyber RAPID initiative and the progress made in building cyber resilience across the region. This initiative underscores Australia's leadership in supporting Pacific partners to meet growing cyber challenges. As this important work continues, there is now an opportunity to extend support beyond training and advisory services to include tangible investments in modernised security operations centres (SOCs), alongside essential hardware and software capabilities.

Pacific nations face increasing exposure to sophisticated cyber threats but often lack the foundational infrastructure required to defend their systems. Providing direct access to secure platforms, trusted technologies and cyber security services – delivered in parallel with ongoing skills development – will significantly strengthen regional resilience. These technologies should be considered the same as other 'infrastructure' and be eligible to be funded in the same way that roads, rail, energy, transport and other infrastructure is funded by donor governments. By supporting digital infrastructure modernization, it will also support Pacific partners to safeguard their sovereignty, protect their citizens and fully participate in the digital economy with confidence.

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?**

Australia should sustain active engagement in UN processes to reinforce norms of responsible state behaviour, while leveraging APEC, the ASEAN Regional Forum and Pacific capacity-building to strengthen resilience and trust in regional digital ecosystems. Similarly, partnerships like the Quad and AUKUS remain critical for coordinating collective responses to emerging cyber challenges. However, we encourage Australia to maintain sustained participation in global standard-setting bodies–including ISO, IEC, ITU, and ETSI. These technical forums are increasingly where the rules of the digital economy are written, shaping the frameworks that underpin cyber, AI and quantum technologies. Without a strong and coordinated Australian presence, our values and interests risk being overshadowed by competing models of governance. The Government should therefore prioritise and resource engagement in these bodies as a core element of cyber diplomacy, ensuring Australia helps set the technical foundations of a secure, open and trusted global digital order.

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

Cisco repeats our input to the 2023 Department of Industry, Science and Resources Consultation on Safe and responsible AI in Australia where any consideration on responsible and secure AI requirements should harmonised and interoperable with internationally recognised standards, to allow Australian and Australia-based enterprises to transact across borders and maintain international competitiveness more seamlessly.

About Cisco and Splunk

Cisco is the worldwide technology leader that securely connects everything to make anything possible. Our purpose is to power an inclusive future for all by helping our customers reimagine their applications, power hybrid work, secure their enterprise, transform their infrastructure, and meet their sustainability goals.

Splunk – a Cisco company – builds a safer and more resilient digital world by helping SecOps, ITOps, and engineering teams keep their organizations securely up and running. In 2024, Splunk was acquired by Cisco to help customers continue to build resilience across their entire digital footprint. Many of the world's largest and most complex organisations trust Splunk to safeguard their mission-critical systems. In Australia, our customers include some of the nation's most important government agencies and critical infrastructure providers—organisations that underpin the country's economic stability, national security, and public safety.