Australia's Cyber Security Strategy 2023 -2030

Horizon 2

Elastic's Submission

elastic.co

Introduction

Elastic is pleased to submit our response to the Horizon 2 Cyber Security Strategy Discussion Paper. As the creators of Elasticsearch and the Elasticsearch Platform, we are a global leader in search-powered solutions that drive core cyber capabilities across security operations and enterprise search.

Elastic is trusted by governments and enterprises around the world to deliver mission-critical outcomes including threat detection, attack surface monitoring, insider risk mitigation, and operational resilience. In Australia, we are proud to support public and private sector organisations in achieving these outcomes through modern, scalable, and open platforms. Our mission is to make data usable in real time and at scale, a principle that aligns closely with Horizon 2's call for faster detection, deeper visibility, and proactive national cyber defence.

A key strength of Elastic is our flexible deployment model. Our platform can be deployed on any major hyperscale cloud provider (AWS, Microsoft Azure, and Google Cloud), on-premises, or in fully air-gapped and classified environments. This flexibility enables agencies and critical infrastructure providers to maintain operational sovereignty and meet data residency, compliance, and security requirements, while benefiting from the same platform innovations available globally.

Elastic is also founded on an open source heritage. We continue to maintain a commitment to openness, transparency, and extensibility through our accessible APIs, open data integrations, and contributions to open standards like OpenTelemetry (OTel). This openness is not just technical, it enables auditability, avoids vendor lock-in, and empowers sovereign capability on a trusted, adaptable foundation.

Our submission outlines how Elastic is investing in key technologies that directly align with the Government's strategic objectives:

- **Generative AI**, embedded into our platform to enhance threat detection, automate investigation workflows, and support cyber teams with natural language insights. Improving response times and helping to scale scarce resources.

- **OpenTelemetry**, to enable vendor-neutral, standardised data collection and unified threat visibility across increasingly complex and hybrid digital environments.

Elastic believes these technologies are critical enablers of the Government's vision for a secure, resilient, and sovereign Australia. We appreciate the opportunity to contribute to this important consultation and welcome ongoing engagement on how industry can best support the Horizon 2 agenda.

Elastic's Responses

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 the Government be exploring for cyber security under Horizon 2?

The coming years will be shaped by widespread and perhaps over-adoption of AI, geopolitical tensions, and the evolving nature of cybercrime. While the proliferation of connected technologies offers economic and digital transformation benefits, they also present a more complex threat environment. The growth in the economic cost of cybercrime, combined with heightened geopolitical competition, require a national cybersecurity posture that is adaptive, resilient, and able to respond quickly to emerging threats.

For Horizon 2, strategic priorities should double down on a security-by-design and security-by-default approach supported by harmonised, streamlined cyber regulation. This would provide clear, low-cost standards, particularly for small-to-medium-sized businesses (SMBs), which remain under-protected and frequent targets. The government should continue positioning Australia as a trusted global cyber leader, working with international partners to strengthen regional resilience. This includes continuing to apply statecraft tools—such as sanctions and advisories—to deter state and non-state actors. Policies must also address risks from emerging technologies, including AI and quantum computing, ensuring that technological progress is balanced with national security and economic stability.

Other key strategic factors for the government to explore include:

Regulatory Harmonisation and Simplification: Elastic recommends a national review to consolidate overlapping cybersecurity obligations across the SOCI Act, Privacy Act, Cyber Security Act 2024, Telecommunications Act (TSSR), APRA CPS 234, and relevant state legislation. These instruments often impose duplicative or conflicting requirements,especially around incident reporting, definitions, and thresholds. The review should also clarify how non-legislative frameworks like the Essential Eight align with regulatory expectations. Greater consistency across laws and standards will reduce compliance burden, improve clarity for industry, and support Horizon 2's goal of a unified and proportionate cyber regulatory environment.

Data Protection: The government should adopt a risk-based, context-driven framework for identifying and protecting valuable datasets. This approach would consider factors like the data's function and sensitivity, rather than just volume or sector, to enable more targeted and proportionate safeguards. The security of data does not depend on its physical location, and mandating data localisation can restrict access to cutting-edge cybersecurity solutions.

Active Cyber Defence: The government should adopt a clearly defined, government-led approach to active cyber defence. Permissible activities should be strictly limited to defensive measures, and private entities should not be empowered to engage in retaliatory actions. To counter advanced cyber threats, especially from nation-states, active cyber defence must integrate AI and machine

learning as core capabilities. These technologies enable automated threat detection, predictive analytics, and real-time response, allowing defences to adapt rapidly to evolving attacks. Without AI, cyber operations risk falling behind adversaries already using these tools at scale.

Vulnerability Disclosures: Promote voluntary, confidential vulnerability disclosure practices aligned with international standards like ISO/IEC 29147 and ISO/IEC 30111. This will encourage broader uptake while preserving operational flexibility and reducing unintended risks.

2.2 Collaborating across all levels of Australian Government

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

The United States Cybersecurity and Infrastructure Security Agency (CISA) offers a model for a “whole-of-nation” approach. This approach provides a blueprint for securing both federal and critical infrastructure by fostering collaboration between public and private sectors, a model that aligns with Australia's strategic goals. One key initiative to adopt is the Zero Trust security framework. This is crucial in today's landscape of hybrid work and multi-cloud environments, where the traditional network perimeter is no longer a sufficient defense.

Elastic supports the CISA Zero Trust Maturity Model by providing a unified data layer that integrates with an organisation's existing technology stack. Elastic's platform ingests, normalises, and analyses data from all Zero Trust pillars including identity, devices, networks, applications, and data enabling comprehensive visibility and real-time threat detection. This capability is essential because without a unified view of all telemetry, an organisation can't effectively "always verify," leaving gaps in its security posture.

Beyond Zero Trust, an Australian equivalent to CISA's free resources and cybersecurity services for state and local government entities would ensure that tools and training are available to all, to improve their security posture. Adopting a joint public-private partnership, similar to CISA's Joint Cyber Defense Collaborative (JCDC), would also enhance large-scale threat information sharing and collaborative defence efforts.

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?

A more refined model should clearly show a feedback loop where outcomes directly influence and adjust interventions. This reflects the agility needed for cybersecurity policy in a rapidly changing threat environment. The model should also define the roles of government, industry, academia, and the community in both implementing measures and collecting the data required to assess results, reinforcing the whole-of-economy and whole-of-nation approach. Lastly, the model should incorporate an explicit feedback loop to demonstrate the dynamic relationship between cybersecurity outcomes, policy interventions and ensuring a continuous cycle of learning and adaptation.

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

Data collection can be strengthened through a federated model, where organisations securely share anonymised telemetry from security tools with a centralised government platform. This would enable a real-time, aggregated view of threats while preserving privacy. Leveraging open standards and common schemas, such as OpenTelemetry (OTel), would ensure consistent analysis across diverse environments.

A national vulnerability disclosure program, similar to the ones promoted by CISA in the U.S. or the Netherlands' Coordinated Vulnerability Disclosure (CVD) policy, could incentivise security researchers to report vulnerabilities. Metrics from such a program covering discovery, reporting, and remediation, could directly inform national cyber risk assessments helping identify systemic weaknesses. Sharing this data with trusted cybersecurity partners would further enhance collective resilience.

The government should also support voluntary, confidential disclosure practices aligned with international standards such as ISO/IEC 29147 and ISO/IEC 30111. Additionally, standardising incident reporting requirements across Five Eyes partners, including aligned definitions, notification timeframes, and data formats, would improve the quality and consistency of information sharing, strengthen national threat intelligence, and reduce compliance complexity for industry.

3.1 Shield 1: Strong businesses and citizens

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.)?

The Government can encourage SMBs and NFPs to use existing cyber resources by increasing visibility through stronger outreach and media campaigns, ensuring that businesses are aware of programs such as the Small Business Cyber Resilience Service, Cyber Wardens, and ACNC guidance. While these programs provide useful guidance, they do not give organisations a clear sense of how their current practices compare to peers or where to start. A simple cyber "health-check" tool could address this gap by providing SMBs and NFPs with a baseline score of their cyber posture. Results could then direct them to the most relevant government or market-based resources, creating a tailored pathway rather than leaving businesses to navigate a fragmented landscape. Elastic's technology could underpin such a tool by securely ingesting incident and configuration data, analysing it in real time, and generating clear, accessible outputs. This approach would complement existing initiatives, help prioritise limited resources, and scale support for the SMB and NFP community.

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?

Not-for-profit entities face distinct cybersecurity challenges that stem largely from their operational and funding structures. Many operate with limited budgets and prioritise service delivery over technology investments, which often results in insufficient security controls. A reliance on volunteers and temporary staff can lead to inconsistent training and gaps in security awareness. Amplifying this structural challenge, many NFPs manage highly sensitive data, such as medical information or records related to vulnerable populations, making them appealing targets for ransomware. The combination of high-value data, limited resources, and irregular workforce continuity creates a heightened risk profile.

To have the greatest impact, government interventions should provide targeted, low-cost, and easily accessible support designed for the realities of the NFP sector. This could take the form of dedicated grant programmes that allow NFPs to implement essential security measures, such as MFA, encryption, and regular patching without drawing funds away from their core mission. The government could also consolidate and simplify existing guidance, such as that from the Australian Charities and Not-for-profits Commission (ACNC), into a single, jargon-free framework tailored for non-technical staff and board members. Additionally, offering sector-specific online training modules, available at no cost, would address the skills gap and foster a stronger culture of security across both permanent and volunteer staff.

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

Protecting against ransomware requires an approach that moves beyond reactive measures to proactive, sustained defence. The Australian Government can strengthen national preparedness through three main areas. First, it can expand proactive programmes that encourage the adoption of essential security controls, offering grants or tax incentives for measures like multi-factor authentication, endpoint protection, secure backup systems, and regular patching particularly for small and medium-sized enterprises (SMEs) that may otherwise struggle to fund such initiatives. These financial supports should be complemented by practical, plain-language resources and free cyber hygiene assessments that help organisations identify gaps and prioritise remediation. Importantly, while insurance can never substitute for robust prevention, it does provide a financial safety net against residual risk, similar to how households both secure and insure their properties. Second, fostering a more integrated public-private threat intelligence ecosystem would significantly improve early warning and coordinated response. While measures such as the Cyber Security Act 2024 have laid the groundwork, additional mechanisms for real-time intelligence exchange between government, critical infrastructure providers, and the wider private sector could enable a faster, more unified defence.

While measures such as the Cyber Security Act 2024 have laid the groundwork, existing mechanisms like the Cyber Threat Intelligence Sharing (CTIS) program provide a starting point for information exchange. However, CTIS participation remains uneven across sectors, and its outputs are often too static or high-level to drive timely defensive actions. Additional mechanisms for real-time,

bidirectional intelligence sharing between government, critical infrastructure providers, and the wider private sector would strengthen situational awareness and enable a faster, more unified defence.

This might include joint operations centers, structured information-sharing agreements, and regular cross-sector exercises to develop rapid decision-making and response capabilities.

Finally, the government can encourage the use of advanced, data-driven security platforms that employ machine learning to detect anomalies indicating a ransomware attack in its earliest stages. Platforms like Elastic can correlate network, endpoint, and user activity to identify suspicious behaviour before it escalates, enabling swift containment and recovery. Promoting these capabilities, alongside traditional security controls, would elevate national resilience and reduce the overall impact of ransomware attacks.

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

Two key regulations significantly reduce cyber risk in Australia: the Security of Critical Infrastructure (SOCI) Act 2018 and the Privacy Act 1988, including its Notifiable Data Breaches (NDB) scheme. The SOCI Act is vital for national security, mandating risk management and timely incident reporting for essential sectors, with penalties to ensure compliance. The Privacy Act focuses on protecting personal information and requires prompt breach notifications to help limit harm from data compromises.

The Essential Eight framework offers a widely recognised baseline for improving cybersecurity maturity across Australian organisations.Though increasingly seen as standard practice, even beyond regulated industries, the framework demands a level of cybersecurity expertise many businesses, particularly SMEs lack. Most cannot afford Managed Service Providers to interpret or implement it effectively.

Elastic's platform helps organisations navigate this complex regulatory environment.Its SIEM and XDR capabilities support real-time incident detection, investigation, and forensic reporting to meet SOCI Act obligations. For Privacy Act compliance, Elastic enables rapid breach detection, scoping, and detailed audit trails. For those adopting the Essential Eight, Elastic supports continuous monitoring of key controls such as application whitelisting, MFA enforcement, and admin privilege restrictions. By centralising visibility across networks, endpoints, and users, the platform both reduces cyber risk and lightens the compliance burden.

However, Australia's cyber regulations remain fragmented**.** Overlapping and inconsistent requirements, such as differing incident reporting timelines under the SOCI Act, Privacy Act, and APRA CPS 234 create confusion and inefficiency. Data retention obligations under the Telecommunications Act can also conflict with privacy laws, while frameworks like the Essential Eight, ISO/IEC 27001, and IRAP vary in scope and assurance levels.

A structured government-led review is needed to streamline these requirements. Consolidating frameworks, aligning definitions, and harmonising thresholds would reduce duplication, lower compliance costs, and let businesses focus more on improving real security outcomes, rather than managing regulatory complexity.

17. Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?

At Elastic, compliance is not seen as a chore, but rather as an enduring strategic advantage. The company adopts a "security by design" philosophy, proactively integrating security and compliance into its operations from the ground up. This approach helps Elastic to not only meet regulatory obligations but also to strengthen its overall security posture and align with industry best practices.

Elastic's platform offers direct support for key Australian cybersecurity mandates, helping businesses meet their regulatory requirements efficiently. For example, its robust encryption, access control, and monitoring features align with the Privacy Act 1988. Similarly, features like asset classification, third-party risk management, and rapid incident reporting help organisations address the requirements of APRA CPS 234. Elastic's monitoring, detection, and control enforcement functions also align with the ASD Essential Eight mitigation strategies, providing a comprehensive solution for managing cyber risks. To further demonstrate its commitment to security, Elastic has achieved IRAO PROTECTED-level assessment for Elastic Cloud on AWS, Google Cloud, and Microsoft Azure in Australia. This achievement allows government agencies and businesses to securely handle sensitive data using the Elastic platform, knowing that it meets rigorous security standards.

While compliance is an important driver of cyber maturity, the current regulatory framework in Australia presents significant challenges. Different obligations are spread across the Privacy Act 1988, the Corporations Act, the Security of Critical Infrastructure Act, and sector-specific instruments such as APRA CPS 234. Even where small and medium-sized enterprises are formally exempt from some of these laws, they often expend time and resources determining whether thresholds apply, mapping overlapping obligations, or preparing for anticipated changes such as the Privacy Act reforms. This complexity creates uncertainty, diverts attention away from genuine cyber risk mitigation, and makes it harder for smaller organisations to engage confidently in the digital economy.

The recently enacted Cyber Security Act was an opportunity to create a more unified and coherent framework. However, it has been criticised for not fully addressing the fragmented nature of the existing laws, leaving businesses to continue navigating a patchwork of different rules and requirements. This underscores the need for a more streamlined and integrated approach to cybersecurity governance 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?

Australia could draw on elements of leading global frameworks to strengthen its secure technology standards. The U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 and the European Union's NIS2 Directive, supported by ENISA, both offer adaptable, risk-based methodologies that emphasise the full lifecycle of cybersecurity functions, identification, protection, detection, response, and recovery. ISO/IEC 27001 also provides an internationally recognised security management standard with a clear path for certification. For operational technology (OT), Critical Infrastructure Resilience (CER), and edge devices, sector-specific frameworks offer more tailored

guidance. The IEC 62443 series is a widely adopted global standard for securing industrial control systems, emphasising defence-in-depth and Cybersecurity Management Systems (CSMS). Singapore's Cybersecurity Act and its Code of Practice for Critical Information Infrastructure (CII) provide another model, mandating clear controls, regular audits, and compliance checks. For edge devices, Australia could integrate secure-by-design requirements with lifecycle management principles from joint guidance issued by the U.S. CISA and NSA, which highlight strong authentication, regular patching, and network segmentation. A tiered national framework, combining NIST CSF and ISO 27001 for broad governance with IEC 62443 and other sector-specific mandates would ensure both general coverage and targeted protection for critical systems.

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?

To better support consumers and end-users in understanding and protecting themselves from cyber threats in their products, the government could enhance collaboration with technology providers like Elastic by leveraging our advanced security platforms. Elastic's AI-powered security analytics and scalable data ingestion capabilities could be utilised to underpin the new smart device labelling scheme, providing real-time insights into product security and informing consumers about potential vulnerabilities. This collaboration could extend to analysing threat data from consumer devices to develop more targeted public advisories and educational content on platforms like cyber.gov.au, ensuring that awareness campaigns such as *Act Now Stay Secure* are data-driven and responsive to emerging threats. Furthermore, Elastic's expertise in secure-by-design principles and its proven compliance with Australian government guidelines, such as its IRAP Protected assessment, could directly contribute to the co-design and refinement of secure product standards, helping to embed robust security into consumer technology from the outset and empowering users with trusted information.

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?

Cyberattacks targeting interconnected data systems can cause cascading effects across multiple industries, even where there is no direct competition. This "trust-innovation dilemma" arises when the need for secure data sharing to drive innovation conflicts with public mistrust and data silos. The government must therefore treat data security as a matter of economic stability as well as national security. International examples, such as NIST CSF 2.0 in the U.S., the EU Data Governance Act, and UK cybersecurity policies, highlight the importance of holistic, enterprise-wide governance that extends beyond technical controls to include supply chain security and executive accountability. Government policy should promote regulatory alignment, harmonised data standards, and open API specifications. Public education campaigns and the use of neutral data intermediaries can help build trust. Incentives for adopting privacy-enhancing technologies and secure data infrastructure should be combined with strong public-private partnerships, such as those modeled on CISA's JCDC, to improve real-time intelligence sharing and coordinated responses.

22. Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed exploited by malicious actors (e.g. IP theft). How does Government and Industry work together to achieve this aim in an evolving global threat environment?

Secure, trusted data sharing between government and industry requires a multi-faceted approach, blending strong public-private partnerships with robust technical and policy measures. Partnerships like the CISA Joint Cyber Defense Collaborative (JCDC) and the NIST Cybersecurity Framework are great examples of how pooling expertise and sharing real-time threat intelligence can enhance security without exposing sensitive information. On the technical side, tools such as secure multi-party computation and data clean rooms allow for collaborative analysis while maintaining privacy. To protect intellectual property, strong access controls, encryption, and secure software development are essential.

From a policy standpoint, governments can establish baseline security requirements, similar to the U.S. Cyber Trust Mark and the EU Cyber Resilience Act. They can also incentivise industry adoption through grants, tax credits, and favourable procurement programmes. Fostering public education and streamlining vulnerability management are also key to reducing overall cyber exposure. Since cyber threats are global, international cooperation through forums like the EU-U.S. Trade and Technology Council and the Five Eyes alliance is critical for aligning standards and coordinating responses.

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

The Australian government should continue to prioritise initiatives that enhance real-time threat intelligence sharing and incentivise the adoption of unified, AI-driven security platforms. The government's commitment to world-class threat sharing and blocking and its investment in sector-specific platforms, such as for the health sector, are crucial steps.This should be expanded by fostering mechanisms for automated, contextualised intelligence exchange, moving beyond static reports to dynamic feeds that can be immediately operationalised by industry. Incentives, potentially through grants or preferred vendor status, could encourage businesses to invest in advanced security solutions capable of ingesting and acting upon this intelligence at speed.

Worldwide, organisations are leveraging Elastic to achieve this scale and speed. A U.S. Public Transit Agency, for instance, dramatically reduced issue resolution time from hours to minutes by unifying data from approximately 20 different security systems and utilising Elastic's ML/AI to filter false positives, particularly for IoT security. Similarly, the Texas A&M University System, which defends tens of thousands of endpoints across universities and state agencies, reduced incident resolution time for phishing campaigns by 99% (from months to hours) using Elastic Security's combined SIEM and endpoint capabilities and automation. This demonstrates Elastic's proven ability to centralise data, automate responses, and empower security teams to block threats effectively across vast and complex environments.

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?

To foster a thriving threat sharing ecosystem in Australia, beyond existing initiatives like the ASD's Cyber Security Partnership Program, Critical Technology and Infrastructure Strategy, and the health sector's dedicated platform, the government needs to champion the widespread adoption of unified,

interoperable security platforms that facilitate real-time, contextualised data exchange. This includes incentivising organisations to centralise their security data and integrate it with national threat intelligence feeds, ensuring that shared information is immediately actionable. Furthermore, establishing clear, standardised protocols for data anonymisation and secure sharing will build trust and encourage broader participation from industry.

While sectors like health already benefit from ISAC structures, additional focus should be placed on areas with both systemic importance and persistent low maturity. Two clear opportunities are education and transport. An Education ISAC could help universities, schools, and training providers address ransomware, phishing, and data exfiltration threats that disproportionately target students and staff. Similarly, a Transport ISAC could provide a coordinated hub for airlines, ports, logistics operators, and local transit agencies to share intelligence on operational technology threats, supply chain disruptions, and cyber-physical vulnerabilities.

For small and medium enterprises (SMEs), a traditional ISAC may be cost-prohibitive. Instead, government could pilot a lightweight “virtual ISAC” model, powered by search and analytics, where anonymised SMB incident data is automatically ingested through a common platform and redistributed back as actionable, sector-relevant alerts. Elastic’s platform is well suited to underpinning this approach by enabling secure, real-time aggregation of diverse telemetry, automated correlation across participants, and simplified dashboards tailored to non-expert users.

These initiatives would not only scale information sharing to more vulnerable sectors but also ensure that insights are delivered in a way that matches each community’s resources and capabilities, moving beyond theory to practical, cost-effective models.

Elastic Security offers a foundational solution to address these challenges and support a thriving ecosystem. Its unified SIEM, XDR, and cloud security platform can ingest, correlate, and analyse petabytes of diverse security data from various sources, making it an ideal central repository for generating actionable threat intelligence. Elastic's flexible hybrid deployment options, including air-gapped environments, and its cost-effective, usage-based pricing model make advanced security accessible to organisations of all sizes, including those in low-maturity sectors with budget constraints or legacy IT. By providing AI and machine learning capabilities that automate tasks and reduce "alert fatigue," Elastic helps overcome the talent shortage, enabling smaller teams to manage larger workloads and contribute more effectively to collective defence, thereby fostering the conditions necessary for new ISACs to thrive.

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

Yes, a unified national VDP would provide consistency and legal clarity for security researchers and organisations alike. While several government agencies have individual VDPs, the absence of a single national framework creates uncertainty, especially in the private sector. A formal program would create a trusted, legal channel for reporting, reducing the risk of legal action against researchers acting in good faith, and encouraging the early identification and remediation of vulnerabilities. Elastic’s architecture is well-suited to support such a program at scale. Its SIEM and XDR capabilities can handle large volumes of incoming reports, integrate them with live threat intelligence, and provide real-time visibility into their potential impact. Automation can streamline the verification and

remediation process, while audit logs and case management functions ensure transparency and accountability throughout the lifecycle of each report.

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 Security of Critical Infrastructure (SOCI) Act is a powerful tool for strengthening Australia's essential services, primarily through its mandatory Positive Security Obligations (PSOs) and Enhanced Cyber Security Obligations (ECSOs). By requiring critical sectors to implement robust risk management programmes and report incidents, the Act compels a significant uplift in security posture. The recent conclusion of grace periods for these obligations, along with the threat of substantial penalties for non-compliance, underscores the government's commitment to enforcement.

While the Act's intent is clear and its enforceability is well-established, there is a need for continuous evolution to ensure its requirements are proportionate and universally understood across the diverse critical infrastructure landscape. The Act's "all-hazards" approach to risk management is comprehensive, but applying these complex requirements to a wide range of operational technology (OT) environments and legacy systems presents challenges for many entities. Ongoing engagement and co-design with industry, as seen with the Horizon 2 consultations, is essential to ensure the obligations remain a realistic and effective measure for all stakeholders, from large corporations to smaller operators within critical supply chains.

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

Owners and operators of critical infrastructure require a coordinated blend of technology solutions, tailored guidance, and targeted incentives to improve resilience. This includes comprehensive asset inventories, exposure management systems, secure access controls for cyber-physical systems, and advanced, real-time threat detection capabilities. While initiatives such as the Critical Infrastructure Uplift Program (CI-UP) are valuable, further support is needed to broaden access and impact. Government can promote adoption by subsidising unified security platforms that provide full visibility across IT and OT environments, offering clear and practical guidance aligned to international standards such as NIST CSF and ISO 27001, and developing sector-specific profiles. Incentives such as grants, tax relief, and preferred procurement status can reward organisations that meet higher security benchmarks. Workforce development programmes—particularly those aimed at OT security—should be prioritised to address the skills shortage.

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

The Australian Government can strengthen private sector engagement with security requirements by focusing on clarity, accessibility, and collaboration. Requirements set out in frameworks such as the Essential Eight and the Information Security Manual (ISM) should be accompanied by practical, plain-language implementation guidance and ready-to-use tools, with consideration given to issuing

contextual guidance by sector. This guidance should acknowledge both the threat vectors in the industry and the relative sophistication of the defences available – both technical and management.

Achieving certifications such as IRAP can be complex, so the government could offer process simplification and even centralised advisory services to reduce administrative overhead for businesses of all sizes. Engagement improves when the private sector is included early in the development and refinement of security policy. A continued “co-design” approach, similar to that taken during Horizon 2 consultations, ensures that requirements are realistic, technologically feasible, and proportionate to the risk.

To further encourage compliance, the government could introduce preferential procurement status for certified vendors, co-funded security uplift programmes, or shared technical services for smaller operators that cannot maintain compliance infrastructure on their own. Elastic’s open-source foundation and transparent detection rules align with these goals by allowing inspection, customisation, and verification critical factors when meeting stringent security standards. Its SIEM and XDR capabilities provide the telemetry, analytics, and reporting needed to demonstrate compliance with technical controls, while flexible hybrid deployment options (including air-gapped and sovereign cloud environments) meet data residency and operational control requirements for sensitive contracts. The S3NS sovereign cloud deployment in France demonstrates how such a model can satisfy both government and regulated-industry requirements for security assurance.

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?

The government's pivotal role in supporting Australia's cyber workforce development and industry growth should be multifaceted, encompassing strategic funding, policy leadership, and fostering robust public-private partnerships. Key initiatives that best support industry growth include the substantial investment in the 'Growing and Professionalising the Cyber Security Industry Program' grant, which aims to establish an industry-led professionalisation scheme, providing clear career pathways and quality assurance for employers. Complementing this, expanding targeted scholarships and apprenticeship programmes, such as those offered by ASD and TAFE institutions, is crucial for attracting diverse talent and building practical skills from early career stages. Furthermore, the government should continue to drive collaborative efforts, like the ASD's Cyber Security Partnership Program and university-industry collaborations, to ensure education and training remain aligned with evolving industry needs and real-world threats, thereby creating a self-sustaining ecosystem of cyber talent.

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?

Effective collaboration depends on breaking down silos and fostering continuous engagement between industry, academia, think tanks, and government. Shared research priorities should be shaped by both current operational needs and long-term strategic goals. A proven model for this is

the creation of joint research and innovation hubs, where funding and leadership are shared, and expertise from different sectors is combined to develop solutions for identified capability gaps.

For meaningful research outcomes, data sharing is essential but must be done ethically and securely. Establishing trusted, secure platforms for anonymised or aggregated data exchange would give researchers access to real-world information without breaching privacy or commercial sensitivities. These platforms could be supported by formal agreements that govern data use and attribution.

Elastic Security's open-source foundation and transparent detection rules make it an ideal platform for collaborative research. Its scalability enables the processing of petabytes of data, while built-in AI and machine learning accelerate the analysis of complex datasets. These capabilities support both academic research and applied projects that can be rapidly operationalised. For example, Georgia Institute of Technology uses Elastic to enhance security analytics and provide researchers and SOC teams with secure access to real-world security data. Similarly, the Texas A&M University System leverages Elastic to drive advanced cyber research and improve visibility across its digital infrastructure. These deployments illustrate how industry-grade tools can bridge research and operational outcomes in support of national cyber resilience.

43. How can government and academia enhance its partnership and promote stronger people-to-people links and collaboration on research and policy development activities?

Building a stronger partnership between government and academia requires institutionalising pathways for ongoing collaboration. A key part of this effort is talent exchange programmes, which allow cybersecurity professionals and policymakers to work within research environments. At the same time, academic experts can contribute directly to policy development. These exchanges foster mutual understanding and ensure that policy is informed by the latest research, and that research is grounded in operational realities.

Joint research centers, or "policy labs," can co-locate academic and government teams to focus on priority areas like critical infrastructure protection, secure AI adoption, and incident response coordination. These centers could host short-term "research sprints" or "policy hackathons" to address pressing challenges. Integrating academics into government training programmes and inviting government experts to lecture in university courses would also help keep curricula aligned with real-world needs.

Elastic can support this collaboration by providing a shared, secure analytical platform where both government and academic researchers can work with real or simulated data. Its open architecture encourages transparency, while its scalability ensures that large, complex datasets such as those generated during cyber exercises or policy simulations can be analysed efficiently.

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?

The most pressing ICT concentration risks emerge when critical services become heavily dependent on a single cloud provider, software vendor, or hardware supplier. These dependencies can lead to cascading failures during an outage, a compromise, or a sudden change in vendor policy. Additionally, over-reliance on proprietary systems can stifle innovation and create long-term migration challenges, locking organisations into a specific technology stack. Similarly, in the supply

chain, an over-reliance on a small number of manufacturers or service providers can introduce systemic vulnerabilities if those suppliers are disrupted or compromised.

Mitigating these risks requires deliberate diversification. Organisations should adopt multi-cloud or hybrid cloud architectures to distribute workloads across different providers. They should also invest in vendor-neutral or open-source solutions that support portability and ensure that clear exit strategies are in place for all critical systems. Continuous vendor risk assessments should be a standard practice to identify weaknesses early, and procurement guidelines should incorporate an analysis of ICT concentration risk into all decision-making processes.

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?

While existing initiatives such as the Southeast Asia and Pacific Cyber Program (SEA-PAC Cyber) and the deployment of Australian cyber security assistance teams have strengthened regional resilience, there is scope for deeper engagement to achieve a fully integrated and sustainable regional security posture. A truly holistic approach requires interoperability of systems, shared operational capabilities, and investment in local expertise across the Indo-Pacific. The government could facilitate the creation of joint regional threat intelligence platforms and fusion centers, moving beyond bilateral exchanges to multilateral, operationally focused hubs. These would enable real-time intelligence sharing and collaborative analysis, supporting faster and more coordinated responses to cyber incidents affecting multiple countries simultaneously. Promoting the adoption of adaptable cybersecurity frameworks, such as tailored profiles of the NIST Cybersecurity Framework would help align security baselines across different jurisdictions, improving interoperability and collective defence.

A major constraint in the region remains the shortage of skilled cybersecurity professionals. Expanding joint training programmes, scholarship opportunities, and exchange initiatives could help address this gap, with a focus on specialist skills such as OT security, incident forensics, and secure software development. Establishing formalised, cross-border incident response protocols and conducting regular multinational exercises would also strengthen the region’s ability to respond to large-scale cyber crises. Finally, Australia could collaborate with regional partners to promote secure-by-design procurement standards and facilitate the transfer of secure, open-source technologies, reducing reliance on proprietary systems that may present hidden vulnerabilities.

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

Beyond its current design and scope of rapid incident response and proactive vulnerability identification, Cyber RAPID could provide additional value by evolving into a more comprehensive regional cyber capacity-building and strategic partnership mechanism. This could involve expanding its mandate to include sustained, hands-on training and mentorship programmes for local cybersecurity professionals in Pacific Island nations, thereby addressing critical skill gaps and fostering self-reliance in incident response and threat intelligence analysis. Furthermore, Cyber RAPID could facilitate the establishment of regional cyber fusion centers, promoting real-time, contextualised threat information sharing and collaborative defence operations across multiple countries, leveraging Australia's expertise in developing secure digital infrastructure and promoting 'secure by design' solutions. This expanded role would not only enhance immediate crisis

management but also contribute to the long-term digital literacy and overall cyber resilience of the Indo-Pacific region.

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's influence on global cyber norms is maximised when it participates in forums that set practical, enforceable standards. The United Nations First Committee and its associated processes, such as the Open-Ended Working Group, have established baseline norms of responsible state behaviour, but progress on implementation and enforcement has been limited. Australia should use its credibility to push these forums toward more concrete outcomes, including greater transparency, capacity-building, and accountability mechanisms.

At the same time, plurilateral groups like the Quad Senior Cyber Group and AUKUS provide opportunities to shape trusted supply chains, critical infrastructure protection, and joint approaches to cyber deterrence. While these initiatives remain at an early stage, they represent a chance for Australia to align with close allies on emerging technologies and operational resilience, complementing broader multilateral efforts.

Priority issues for Australia should include advocating for secure-by-design principles in all new technologies,particularly in IoT,to reduce systemic vulnerabilities at scale. The rapid adoption of artificial intelligence also demands international norms governing its ethical and responsible use in cybersecurity, ensuring that AI enhances defence without enabling malicious activity. Another critical priority is creating operational standards for seamless, contextualised threat intelligence sharing between nations, enabling collective, real-time defence against transnational cybercrime and state-sponsored attacks. These standards should be paired with mechanisms to ensure that shared intelligence can be immediately operationalised across jurisdictions. Australia could also champion greater transparency and accountability in incident response, including the establishment of no-fault international review boards to analyse significant breaches and share lessons learned globally.

Elastic's open-source architecture and transparent detection rules align with these priorities by enabling inspection, customisation, and trust in security technology. Its AI and machine learning capabilities demonstrate how advanced tools can be responsibly integrated into defensive operations, and its federated search capabilities proven in sovereign cloud deployments like S3NS in France, provide a practical model for enabling world-class threat sharing without compromising national data sovereignty.

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

Two areas deserve special attention. First, Australia should continue to advocate for the widespread adoption of secure-by-design requirements for all new technologies, particularly for IoT devices. This would address systemic risks that transcend borders. Second, it should champion harmonised approaches to mandatory ransomware reporting. This would include clear "limited-use" provisions for shared incident data, which would encourage transparency without fear of punitive consequences. These actions would promote consistent global threat intelligence exchange, improving nations' collective ability to respond to emerging threats.

The government should also prioritise pursuing mutual recognition of cloud security certifications by mapping functionally equivalent controls across international frameworks. This would promote interoperability, strengthen cyber resilience, and ensure that Australia remains a leading voice in shaping trusted, globally integrated digital ecosystems. Elastic Security is well-suited to support the operationalisation of these international frameworks. Its unified SIEM, XDR, and cloud security capabilities provide the necessary data ingestion, analytics, and automated response functions to implement core NIST and ISO requirements. Its open-source transparency supports secure-by-design principles, and its ability to integrate diverse threat intelligence feeds ensures that shared data is actionable in real time.

The point of contact for this response is: