infotrust

SECURE YOUR FUTURE.

PUBLIC SUBMISSION: DEVELOPING HORIZON 2 OF THE 2023–2030 AUSTRALIAN CYBER SECURITY STRATEGY

Response to Public Consultation Paper

Prepared for Department of Home Affairs
Public Submission
August 2025

Contents

1. Executive Summary

Australia's cyber resilience in Horizon 2 depends on moving from fragmented, reactive measures to a unified, proactive, and globally aligned approach. This requires simplifying compliance, consolidating frameworks, uplifting critical infrastructure, empowering businesses and citizens, and strengthening sovereign capabilities. By embedding security into every layer of the economy and aligning with international best practices, Australia can achieve systemic resilience and maintain its position as a trusted global cyber leader.

Developing our vision for Horizon 2

Outlook for Horizon 2

Horizon 2 represents a critical transition from tactical responses to strategic resilience. The focus must be on establishing a unified national cyber security framework anchored in the ISM, supported by published crosswalks to elements such as: NIST CSF 2.0, ISO/IEC standards, GDPR, SOC 2, HIPAA, PCI DSS, and AI RMF. National risk tolerance should be defined centrally, with consistent privacy obligations applied across all sectors. Enforcement must be consistent across government, private sector, and SOCI entities, supported by incentives and proportionate penalties. At the same time, emerging risks such as ransomware, supply chain vulnerabilities, and the security of operational technology, IoT, and critical energy resources must be addressed. Building sovereign capabilities in workforce, technology, and research will also reduce strategic dependencies and foster innovation.

Collaborating across all levels of Australian Government

Fragmentation across federal, state, and local jurisdictions creates systemic vulnerabilities and inefficiencies. A coordinated, multi-jurisdictional approach is essential to unify objectives, reduce duplication, and enable knowledge sharing. Aligning state and territory initiatives with national strategies will ensure policy coherence and consistent implementation. This collaboration should extend to joint exercises, shared threat intelligence, and harmonised regulatory expectations, ensuring that all levels of government work toward common security outcomes.

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

As the threat landscape evolves, measuring progress requires a dynamic and adaptable evaluation model. The framework should embed feedback loops to ensure continuous improvement and relevance, while simplifying complexity by clarifying roles and responsibilities. Data-driven insights must be leveraged to monitor engagement, adoption, and incident trends. Participation should be broadened by reducing barriers to feedback, enabling anonymous contributions, and promoting inclusivity across sectors. Transparent reporting on sector-specific outcomes and national resilience metrics will inform policy adjustments and maintain accountability. A simplified, transparent model supported by inclusive feedback mechanisms will ensure that cyber security outcomes remain measurable, actionable, and aligned with national objectives in an increasingly complex environment.

Shield-level focus for Horizon 2

Shield 1: Strong businesses and citizens

Public awareness is fragmented; create a national cyber awareness hub to unify messaging, using data-driven campaigns and trusted advocates. Simplify access for SMBs and NFPs with incentives, peer models like Cyber Wardens, and advisory support. Enhance shared services, vulnerability monitoring and breach alerts and set stronger supply chain requirements. Combat ransomware with targeted education, funding, standard clarity, and better professional certifications. Streamline standards by using ISM and crosswalks to reduce duplication.

Shield 2: Safe technology

Secure the growing estate of edge devices, OT, and critical energy resources. Publish OT-specific guidance within ISM and set practical approaches for legacy systems. Partner with ISPs to improve consumer device security through secure defaults, lifecycle updates, and clear guidance. Establish frameworks and guidance to assess foreign ownership and influence risks. Provide centralised, actionable guidance for emerging technologies that reflects the speed and scale of modern exploitation.

Shield 3: World-class threat sharing and blocking

Define and publish a proactive posture for industry with measurable objectives. Deliver economy-wide controls by offering a public DNS service with safe browsing warnings and sharing indicators of compromise in usable formats. Run joint exercises to clarify roles, decision points, and communications in crisis. Incentivise vulnerability disclosure policies and establish a national program supporting verified anonymous reporting to accelerate remediation.

Shield 4: Protected critical infrastructure

The SOCI framework lacks proportionality and is subject to inconsistent interpretation. Integrate CIRMP expectations with ISM rather than layering frameworks and expand coverage to essential entities currently excluded but posing systemic risk. Close the third-party gap by requiring risk management for contractors and managed providers with privileged access. Reduce regulatory burden through consolidation of standards and published crosswalks, and increase assurance through targeted audits, incentives, and penalties calibrated to risk.

Shield 5: Sovereign capabilities

Grow a skilled and diverse workforce through an expanded TAFECyber pathway integrated with university programs and a national professional registration model similar to chartered status. Create targeted mid-career transitions from system administration, audit, legal, HR, safety, and project management. Partner with ACS for scalable training and recognition. Prioritise sovereignty in sectors with concentrated ICT risk such as healthcare, real estate, and building management, using certification, uplifted data handling standards, and focused SMB enablement.

Shield 6: Strong region and global leadership

Align Australian compliance requirements with widely recognised global frameworks to facilitate international operations. Establish a central control set for information security management, maintaining crosswalks and a process for new mappings. Strengthen regional capabilities through intelligence sharing, readiness exercises, and technical support, and apply diplomatic advisories and joint statements to address threats.

2. Response to Developing our vision for Horizon 2

2.1 Outlook for Horizon 2

As Australia enters Horizon 2, the national cyber security strategy must evolve from short-term, tactical responses to a more systemic and coordinated approach. The current environment is characterised by fragmentation, where agencies, sectors, and businesses operate under different standards and risk tolerances. These risks will intensify as digital interdependencies deepen, and emerging technologies such as artificial intelligence and quantum computing accelerate the complexity and speed of cyber threats.

To address these challenges, a unified and enforceable cyber security framework is essential. Such a framework will provide clarity, reduce compliance complexity, and ensure that all organisations, regardless of size or sector, operate to a consistent baseline of security.

Standardisation Across Sectors
A single baseline security framework should apply to government, private sector, and critical infrastructure. This framework should align with established standards such as the Information Security Manual (ISM) and the Essential Eight, while providing comparable controls and clear mappings to international frameworks like NIST and ISO which are discussed in the *Shield 6: Strong region and global leadership* portion of this response paper. Harmonising these standards will reduce compliance complexity and support interoperability across industries.

Centralised Risk Governance
Risk tolerance should be defined at a national level rather than by individual agencies or organisations. A central authority should set and maintain these parameters, e.g. Australian Signals Directorate, Finance, Home Affairs, National Cyber Security Coordinator. Similarly, privacy and data protection obligations must be applied uniformly, ensuring that SMBs and large enterprises meet the same baseline requirements. Regardless of who holds the data, its value to a cyber adversary remains the same.

Consistent Enforcement and Accountability
A single enforcement model should span relevant government, public, private, and SOCI sectors. This could include mandatory reporting, independent audits, and proportionate penalties for non-compliance. Incentives for proactive security measures can further drive continuous improvement and uplift across the ecosystem.

A unified approach in Horizon 2 will deliver predictable security outcomes, reduce duplication and compliance burden, and strengthen resilience across interconnected sectors, laying the foundation for Horizon 3 and beyond.

2.2 Collaborating across all levels of Australian Government

Australia's cyber security governance is currently challenged by fragmentation across federal, state, and local jurisdictions. Each level of government often operates under different standards, risk tolerances, and program priorities, creating inefficiencies and systemic vulnerabilities that adversaries can exploit. This lack of cohesion also limits the ability to share knowledge effectively and scale successful initiatives nationally.

Rather than replicating individual state or territory programs, the strategic priority should be aligning these initiatives with national frameworks to ensure policy coherence and reduce duplication. Such alignment enables structured knowledge exchange, optimises resource allocation, and addresses critical challenges such as the cyber skills shortage. By operating under shared objectives and consistent standards, governments can collectively enhance capability development, minimise knowledge silos, and strengthen the resilience of Australia's cyber ecosystem.

A unified, collaborative approach across all levels of government is essential to achieving a secure, coordinated, and future-ready national cyber security posture.

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

As the cyber threat landscape evolves, measuring progress and ensuring accountability becomes increasingly complex. Traditional evaluation models often fail to keep pace with rapid technological change and shifting risk environments. Without a clear and adaptable framework, there is a risk that cyber security initiatives will lose relevance, lack measurable impact, and fail to inform future policy decisions effectively.

The proposed high-level model provides a strong foundation, particularly in recognising the importance of feedback loops for continuous improvement. Feedback mechanisms are essential to ensure that the model remains dynamic, responsive, and aligned with emerging threats. However, the current model appears overly complex, which may hinder adoption and create ambiguity around roles and responsibilities. Simplification is necessary to make the framework more accessible and actionable for stakeholders across government and industry.

To support this, robust mechanisms for collecting data and feedback must be embedded within the model. Industry awareness of existing programs, such as the ACSC partnership, remains limited, reducing participation and the quality of insights gathered. Increasing visibility of these programs and lowering barriers to entry, such as the requirement for director-level sign-off, would encourage broader engagement. Introducing flexible delegation options and enabling anonymous feedback from cyber security professionals, even those outside formal partnerships, would further enhance inclusivity.

These measures would ensure that valuable expertise is not lost when individuals change roles or organisations, preventing fragmentation of industry knowledge.

A simplified, transparent model supported by inclusive and accessible feedback mechanisms will enable continuous improvement, strengthen stakeholder engagement, and ensure that cyber security outcomes remain measurable and relevant in a rapidly changing world.

3. Response to Shield-level focus for Horizon 2

3.1 Shield 1: Strong businesses and citizens

Australia's cyber resilience relies heavily on the security practices of businesses, non-profit organisations (NFPs), and individuals. However, awareness and adoption of cyber security measures remain inconsistent, particularly among small and medium-sized businesses (SMBs) and NFPs. These entities often face resource constraints, lack technical expertise, and struggle to navigate complex standards and fragmented messaging. At the same time, individuals and smaller organisations are increasingly targeted by sophisticated threats such as ransomware, which has evolved into a highly organised and commercialised criminal enterprise. Without a coordinated approach to awareness, education, and support, these vulnerabilities will continue to undermine national security and stability.

Government messaging on cyber security is currently dispersed across multiple agencies, levels and platforms, creating confusion and reducing impact. A unified national cyber awareness framework is needed to align messaging across federal, state, and local levels. Establishing a single authoritative portal that consolidates resources from agencies such as ACSC, Home Affairs, and CISC, among others, would provide a trusted source of information, including educational content, alerts, and reporting guidance. Campaigns should leverage trusted messengers such as community leaders and industry bodies, use real-life examples to make risks relatable, and apply data-driven strategies to target high-risk groups. Integrated, multi-channel campaigns and interactive workshops can further reinforce key messages.

Encouraging SMBs and NFPs to adopt existing cyber resources requires simplifying access and messaging, integrating cyber guidance into business registration and compliance processes, and leveraging trusted networks such as industry associations and local councils. Incentives such as grants, cyber insurance discounts, and recognition programs can motivate participation. Tailored resources for non-technical users, combined with peer-to-peer models like Cyber Wardens, will make adoption practical. Additional measures could include free consultations, director engagement sessions, and embedding cyber awareness into business-as-usual processes.

Industry and government collaboration is essential to co-design practical resources and training tailored to SMB and NFP needs. Coordinated messaging between government and industry will avoid duplication and confusion, while sharing success stories will build trust and demonstrate impact. Supply chain security should be strengthened by introducing minimum cyber maturity requirements for government tenders and subcontractors.

Providing free vulnerability monitoring services and breached credential alerts can significantly lower the barriers for small and medium-sized businesses (SMBs) and not-for-profits (NFPs) to participate in proactive cyber security. These services enable organisations to identify exposures, such as unpatched systems or compromised credentials, before they are exploited,

without the need for in-house expertise or costly third-party solutions. By receiving timely alerts about vulnerabilities and breaches, businesses can take immediate action to mitigate risks, reducing the likelihood and impact of cyber incidents.

In parallel, enhancing risk awareness through the use of financial impact modelling tools will empower organisations to make informed decisions about cyber investment. By quantifying the potential costs associated with cyber incidents, such as business interruption, regulatory penalties, and reputational damage, these models help business leaders understand the return on investment for security controls and justify expenditure to boards and stakeholders. This dual approach not only improves baseline security across the economy but also supports a more mature, risk-based culture where cyber security is viewed as a strategic business enabler rather than a compliance burden.

The ransomware threat continues to evolve and is driven by Ransomware-as-a-Service, targeted attacks, and the use of AI for phishing and lateral movement. The attack surface has evolved and now includes cloud services, third-party providers, and even cyber physical systems expanding into homes where they historically have been isolated to industrial settings. To address these evolving threats, government should deliver both financial and technical support to uplift baseline cyber security across the economy. This could include targeted grants or subsidies for essential security tools, subsidised training programs, and tailored advisory services, particularly for small and medium-sized businesses and not-for-profits that may lack internal resources. Public awareness campaigns should be strengthened and adapted to reach diverse audiences, using language, channels, and examples that resonate with different demographics and levels of digital literacy.

In parallel, regulatory measures must keep pace with the threat landscape. This includes introducing clear requirements for cryptocurrency exchanges to prevent their misuse in cybercrime, enhancing supply chain security through enforceable standards for third-party providers, and mandating minimum security controls across all sectors. Finally, uplifting the quality and accessibility of professional certification schemes, and investing in multilingual and culturally inclusive cyber education, will help build a more resilient and diverse workforce, ensuring that all Australians are equipped to recognise and respond to cyber risks.

Though it can be tempting to introduce new standards, regulations, or frameworks in response to emerging threats, doing so often adds unnecessary complexity and creates confusion for organisations already struggling to meet existing requirements. Instead, the focus should be on consolidating and harmonising the frameworks we already have in order to create a more streamlined and practical approach to cyber security.

Australia has strong foundations in the Information Security Manual (ISM) and the Essential Eight, which provide clear, actionable guidance for improving security posture. These should remain the cornerstone of national cyber security standards, supported by published crosswalks that map their relationship to widely recognised international frameworks such as the NIST

Cyber security Framework (NIST CSF) and ISO 27001. These mappings will help organisations understand how implementation of one framework contributes to meeting the requirements and intentions of others, reducing duplication and easing the burden on resource-constrained entities such as SMBs and NFPs. Clear guidance on when and how to apply each framework based on organisational size, sector, and risk profile is essential. This approach would provide a single source of truth while maintaining interoperability for organisations operating in global markets.

In short, building strong businesses and informed citizens requires a unified approach that combines clear messaging, practical support, and collaborative partnerships. By simplifying standards, incentivising adoption, and addressing emerging threats, Australia can create a resilient cyber ecosystem where every organisation and individual contributes to national security and resiliency.

3.2 Shield 2: Safe technology

As Australia accelerates its adoption of digital technologies, the security of edge devices, operational technology (OT), and critical energy resources (CER) becomes increasingly critical. These technologies underpin essential services and industrial processes, yet they often operate with outdated security measures or lack consistent standards. The rapid integration of Internet of Things (IoT) devices and emerging technologies further expands the attack surface, creating new vulnerabilities that adversaries can exploit. Without a clear and unified approach to securing these technologies, Australia risks systemic weaknesses that could impact national security, economic stability, and public safety.

To address these challenges, Australia should prioritise enhancing existing frameworks rather than introducing new ones. Incorporating specific guidance for OT within the Information Security Manual (ISM) which would ensure that critical systems are aligned with nationally. This guidance should include strategies for protecting legacy OT systems, which are often difficult to patch, as well as requirements for securing future deployments. Establishing a clear cutoff point for legacy systems and providing practical hardening measures will help organisations manage risk effectively.

Consumer protection also requires a strong partnership between government and Internet Service Providers (ISPs) to improve the security of default devices such as home routers, which often serve as the first line of defence for households and small businesses. These devices are frequently deployed with minimal security measures, making them an attractive entry point for attackers seeking to compromise home networks and launch broader attacks.

To address this, Government should work with ISP's to ensure that devices are delivered with secure configurations from the outset and that security updates are applied consistently throughout the device lifecycle. This collaboration should also include providing clear, accessible guidance to consumers on how to maintain device security. Many users lack the technical knowledge to identify risks or apply best practices, so practical, easy-to-understand

resources are essential. ISPs could also offer user-friendly tools that help customers monitor device health and receive alerts about potential issues.

Managing foreign ownership, control, or influence (FOCI) risks in technology supply chains is another critical priority. Clear risk frameworks and assessment processes should be developed to help organisations identify and mitigate potential vulnerabilities associated with foreign vendors. These frameworks must be practical, transparent, and adaptable to evolving geopolitical risks.

Building a secure technology ecosystem requires more than isolated measures; it demands a coordinated national approach that integrates strong standards, practical guidance, and shared accountability. By consolidating existing frameworks, embedding clear requirements for operational technology and critical energy resources, and adopting proven international practices such as the existing IoT security labelling schemes, Australia can create a consistent and trusted security baseline.

Finally, the government should provide centralised, accessible guidance for the safe adoption of critical and emerging technologies. This guidance should emphasize the speed and scale of exploitation in modern threat environments, helping organisations understand the urgency of implementing robust security measures. By highlighting these risks and offering actionable recommendations, the government can drive proactive security practices across all sectors.

Strengthening partnerships with ISPs to improve consumer device security, addressing supply chain risks through transparent risk frameworks, and providing centralised guidance for emerging technologies will further reduce systemic vulnerabilities. Through these combined efforts, Australia can ensure its technology infrastructure remains resilient, secure, and capable of supporting innovation in an increasingly complex threat environment.

3.3 Shield 3: World-class threat sharing and blocking

Australia's ability to defend against cyber threats depends on a proactive, collaborative approach between government and industry. However, the current posture is largely reactive, with fragmented standards, inconsistent threat-sharing practices, and limited mechanisms for coordinated response. This creates systemic vulnerabilities that adversaries can exploit at scale.

To build a truly resilient cyber ecosystem, Australia must define and operationalise a proactive security posture that empowers industry, enhances intelligence sharing, and enables threat blocking at scale.

Government can support industry by simplifying compliance and making security easier to implement. Consolidating legislation and policies and providing clear crosswalks between domestic and relevant international standards such as ISM, Essential Eight, ISO 27001, and NIST CSF, will reduce complexity and align Australia with global best practices. When security requirements are clear and practical, businesses are more likely to adopt them as part of their standard operations.

Defining what a proactive cyber security posture looks like for industry is essential, clear targets help guide organisations in uplifting their security maturity, as voluntary improvements are less likely to occur in the absence of defined objectives and best practices. Establishing measurable objectives and baseline expectations will provide a structured framework for businesses to follow, ensuring alignment with national priorities and improving overall resilience.

Blocking threats at scale requires government-led initiatives that deliver shared protections across the economy. Implementing a public DNS service with built-in threat blocking and safe browsing warnings would provide an additional layer of defence for all users, reducing exposure to phishing, malware, and other online threats. Making Indicators of Compromise (IOCs) readily available to industry will further enhance detection and response capabilities, enabling organisations to act quickly against emerging threats.

Preparedness for cyber conflict or crisis scenarios remains low, and roles and responsibilities between government and industry are not clearly defined. To address this, government should conduct joint cyber exercises with industry participation, simulating real-world attack scenarios to test decision-making, communication protocols, and escalation pathways. These exercises will help identify gaps, clarify responsibilities, and ensure that both sectors can respond effectively under pressure.

Finally, fostering a culture of responsible vulnerability management is critical. Government should incentivise businesses to adopt vulnerability disclosure policies through a combination of rewards and requirements, such as incentives for maintaining security baselines with external assurance and establishing a national vulnerability disclosure program that allows verified but anonymous reporting will encourage security researchers to share findings without fear of legal repercussions, improving the speed and effectiveness of remediation.

Building a world-class threat-sharing and blocking ecosystem requires clarity, collaboration, and shared accountability. By defining a proactive posture, simplifying compliance, enabling large-scale threat blocking, and strengthening intelligence sharing, Australia can create a cyber defence model that is both adaptive and resilient in an evolving threat landscape.

3.4 Shield 4: Protected critical infrastructure

Australia's critical infrastructure underpins essential services such as energy, healthcare, transport, and communications. However, the current regulatory framework, including the Security of Critical Infrastructure (SOCI) Act, is not delivering the level of protection required to address today's complex and evolving threat landscape. Obligations are often poorly understood, inconsistently applied, and in some cases, not proportionate to the risks they aim to mitigate. This lack of clarity and uneven compliance creates systemic vulnerabilities that adversaries can exploit, with potentially severe consequences for national security, economic stability, and public safety.

The SOCI Act mandates the implementation of a Critical Infrastructure Risk Management Program (CIRMP), but this requirement is widely misunderstood and perceived as yet another

layer of complexity. Rather than introducing additional frameworks, the government should integrate requirements into existing standards, similar to the approach used for Defence Industry Security Program (DISP) membership. Streamlining implementation in this way would help reduce duplication and administrative burden for regulated entities. Additionally, the current scope of the SOCI framework does not extend to some essential service providers, such as hospitals without intensive care units and certain supply chain entities supporting critical infrastructure, like energy metering providers. Addressing these exclusions by broadening the definition of critical infrastructure would help close important gaps in national resilience.

Supply chain risk remains one of the most significant blind spots in the current framework. While SOCI requires reporting for data storage and processing, it does not adequately address risks associated with contractors, managed service providers (MSPs), and other third parties with privileged access. These entities often represent the weak link in the security chain and must be brought under a consistent risk management oversight. Clear guidance and enforceable requirements for third-party risk management are essential to closing this gap.

The regulatory burden on industry is not proportionate to the outcomes being sought. Complexity and misalignment across multiple standards make compliance difficult and costly, without necessarily improving security. Consolidating frameworks, such as integrating the Essential Eight within the ISM and providing published crosswalks to international standards like NIST CSF, would simplify compliance while driving greater awareness of critical controls. This approach would reduce duplication, improve clarity, and ensure that security uplift efforts deliver measurable results.

To support critical infrastructure owners and operators in maturing their cyber and operational resilience, the government should provide simplified requirements with clear objectives, supported by practical tools and guidance. Centralised resources that map obligations across frameworks, combined with incentives for compliance and penalties for non-compliance, will drive consistent implementation. Regular joint exercises between government and industry should also be conducted to test crisis response capabilities, clarify roles and responsibilities, and ensure readiness for cyber conflict or major incidents.

Finally, the government must strengthen engagement with private sector partners by centralising security requirements and aligning them with best practices. Current adoption of government frameworks among private sector entities remains inconsistent, often due to perceptions of irrelevance or excessive complexity. By making requirements clearer, more accessible, and aligned with operational realities, the government can foster greater collaboration and compliance.

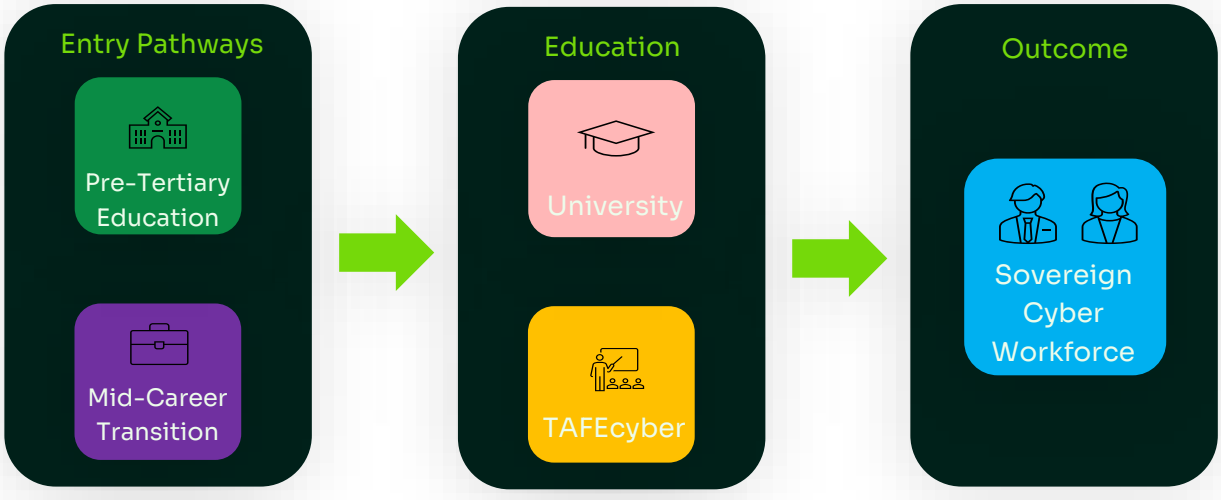
Protecting critical infrastructure requires a unified, risk-based approach that addresses regulatory complexity, closes supply chain gaps, and ensures consistent implementation across all sectors. By simplifying obligations, expanding coverage, and enabling practical support, Australia can build a resilient critical infrastructure ecosystem capable of withstanding the challenges of an increasingly hostile cyber environment.

3.5 Shield 5: Sovereign capabilities

Australia's ability to maintain a secure and resilient digital environment depends on developing sovereign capabilities, particularly in the areas of workforce, technology, and critical ICT infrastructure. However, the current cyber workforce pipeline is insufficient to meet growing demand, and the country remains heavily reliant on foreign technologies and service providers. These dependencies create strategic vulnerabilities that adversaries can exploit, while also limiting Australia's capacity to innovate and respond to emerging threats.

The government plays a central role in addressing these challenges by fostering a skilled and diverse cyber workforce. Programs such as TAFECyber represent a strong starting point, but they must be expanded and integrated into a broader national strategy. This includes embedding vocational cyber training within university degrees to create seamless pathways from technical education to higher education, ensuring graduates possess both practical and theoretical expertise. Additionally, introducing a professional registration scheme similar to the UK's Chartered Cyber Security Professionals would formalise recognition of skills, enhance credibility, and establish clear career progression for cyber security professionals in Australia.

Mid-career transitions and diversity initiatives are also effective pathways to close the workforce gap. Industries such as IT system administration, compliance-heavy sectors (e.g., auditing, legal, HR), and risk management offer highly transferable skills that can be leveraged to strengthen the cyber workforce. Government and industry should collaborate to create targeted programs that retrain professionals from these sectors, supported by incentives and partnerships with organisations like the Australian Computer Society (ACS) and Australian Information Security Association (AISA).



Beyond workforce development, Australia must identify and prioritise sovereign capabilities in critical technology areas. Heavy reliance on foreign ICT solutions in sectors such as healthcare, real estate, and building management systems introduces systemic risks. For example,

healthcare systems depend on integrated technologies for sterilisation, clinical AI, and building management, while real estate platforms handle large volumes of sensitive personal data. These concentrations of risk require targeted mitigation strategies, including certification requirements for ICT systems, stricter data handling standards, and enhanced cyber awareness programs for small and medium-sized businesses operating in these sectors.

Building sovereign capability also requires investment in research and innovation. Government, academia, and industry must collaborate to set research priorities that align with national security objectives and economic growth. This includes fostering partnerships that promote knowledge sharing, joint development of emerging technologies, and commercialisation pathways for Australian-developed solutions.

Strengthening sovereign capabilities is essential to reducing strategic dependencies, closing workforce gaps, and ensuring that Australia can maintain control over its critical digital infrastructure. By investing in education, professional standards, and domestic innovation, Australia can build a secure, self-reliant, and future-ready cyber ecosystem.

3.6 Shield 6: Strong region and global leadership

Australia's ability to lead in global cyber governance depends on shaping international norms, strengthening regional partnerships, and aligning with globally recognised standards. While attributions, advisories, and sanctions remain effective tools for signalling accountability and building awareness, they must be complemented by a broader suite of diplomatic, regulatory, and operational measures to counter increasingly sophisticated cyber threats.

Defining a proactive cyber diplomacy posture for Horizon 2 is essential. Australia should actively participate in international forums to influence the development of rules, norms, and standards that align with national interests. Priority areas include data protection, supply chain security, and emerging technologies such as artificial intelligence and quantum computing. Engagement should focus on harmonising regulatory frameworks with key partners and promoting interoperability through alignment with globally recognised standards and frameworks, including but not limited to:

- General Data Protection Regulation (GDPR) for data privacy and protection.
- SOC 2 for security, availability, and confidentiality in service organisations.
- NIST Cyber security Framework (CSF 2.0) and NIST AI Risk Management Framework (AI RMF) for comprehensive governance of cyber and AI-related risks.
- HIPAA for sensitive healthcare data.
- Payment Card Industry Data Security Standard (PCI DSS) for securing financial transactions.
- ISO/IEC standards, including:

- ISO/IEC 27001 for information security management.
- ISO/IEC 27701 for privacy information management.
- ISO/IEC 62433 for secure product lifecycle and supply chain security.
- ISO/IEC 42001 for AI management systems.

Domestically, Australia must simplify compliance for organisations operating globally by consolidating local frameworks and publishing crosswalks to these international standards. The Information Security Manual (ISM) should serve as the central reference point, with mappings to frameworks such as NIST CSF, ISO standards, SOC 2, HIPAA, and PCI DSS. This approach would reduce duplication, improve clarity, and position ISM as the single authoritative control set, enabling organisations to meet both domestic and international obligations efficiently. A formal process for requesting new crosswalks should also be established to ensure the ISM remains current and adaptable as global standards evolve.

Building a strong regional and global leadership position requires more than alignment; it demands active participation in shaping the future of cyber governance. By harmonising standards, consolidating domestic frameworks, and leveraging diplomatic and operational tools, Australia can lead by example and ensure that its values of security, trust, and openness underpin the global digital ecosystem.

4. Additional Response

As Australia moves into Horizon 2, it is essential to ensure that cyber security obligations are clear, consistent, and achievable for all organisations, regardless of size. Data security must not be treated as optional for small businesses or non-profit entities; the value of data to adversaries remains the same regardless of who holds it. However, the cost and complexity of compliance often present significant challenges for smaller organisations, reducing these barriers while maintaining robust security outcomes is critical.

Setting minimum standards that are simple, accessible, and enforceable will help create a level playing field. These standards should be aligned across key regulatory and industry bodies such as but not limited to: ASIC, APRA, Home Affairs, ASD, and AICD to ensure consistency and avoid duplication. A unified approach will prevent fragmentation, where agencies and sectors operate under different interpretations of security requirements. Accountability mechanisms must also be strengthened so that compliance is not left to voluntary interpretation.

Awareness of the Information Security Manual (ISM) should be prioritised over separate promotion of the Essential Eight (E8). Positioning ISM as the central reference point, with E8 integrated as a core component, will create a more cohesive and comprehensive security

framework. This approach will also help organisations understand the broader set of controls beyond E8, which are often overlooked when treated as standalone requirements.

Support for individuals is equally important. There should be a clear pathway for consumers to access cyber security assistance, including an expanded role for ACSC or a similar entity dedicated to public engagement. With the rise of AI-driven tools and low-code or "vibe coding" applications, the barrier to entry for malicious actors has dropped significantly. Activities once limited to advanced threat actors can now be executed by less skilled individuals, increasing the risk of opportunistic attacks. Understanding these evolving motivations and behaviours is essential for designing effective awareness and prevention strategies.

Finally, practical tools should be developed to help organisations navigate compliance obligations. Flowcharts and decision trees can simplify complex requirements, while interactive tools, similar to the Fair Work Award Finder, could provide tailored guidance based on organisational characteristics. These tools would not replace legal advice but would offer high-level clarity, reduce confusion and improve compliance outcomes.

Building a secure and resilient cyber ecosystem requires clarity, accessibility, and accountability. By simplifying standards, aligning regulatory expectations, and providing practical support for both organisations and individuals, Australia can ensure that cyber security becomes an achievable and integral part of every entity's operations.

5. Conclusion

Infotrust welcomes the opportunity to contribute to the Horizon 2 phase of the 2023–2030 Australian Cyber Security Strategy and commends the Government's continued leadership in strengthening Australia's digital resilience. We also thank the Department of Home Affairs for engaging industry early in the consultation process. Being involved at this stage is critical and represents a significant step forward for the nation, ensuring that policy settings are informed, practical, and aligned with real-world challenges.

As a sovereign Australian cyber security provider with a world-class Security Operations Centre and a proven track record in protecting organisations across sectors, Infotrust is deeply invested in advancing national cyber maturity. We strongly support the Strategy's focus on empowering small businesses, uplifting critical infrastructure, harmonising regulation, and fostering sovereign capability to drive whole-of-economy resilience.

Our submission emphasises the need for a unified and enforceable cyber security framework, consolidation of standards, and practical mechanisms for compliance to reduce complexity and improve adoption. We advocate for stronger collaboration across all levels of government, industry, and academia to address systemic vulnerabilities, uplift workforce capability, and ensure that security measures are proportionate, accessible, and effective.

We also highlight the importance of international alignment through harmonization with globally recognised frameworks such as GDPR, SOC 2, NIST CSF 2.0, NIST AI RMF, HIPAA, PCI DSS, and ISO/IEC standards (27001, 27701, 62433, and 42001). This alignment, combined with published crosswalks and a centralised reference point in the ISM, will simplify compliance and position Australia as a global leader in cyber security governance.

Finally, we stress the urgency of addressing emerging risks, including ransomware, supply chain vulnerabilities, and the security of operational technology, IoT, and critical energy resources. Building sovereign capabilities, strengthening regional partnerships, and leveraging diplomatic tools will be essential to maintaining trust, resilience, and leadership in an increasingly contested digital environment.

Infotrust remains committed to continuous threat exposure management, proactive defence, and tailored consulting that aligns technical rigor with strategic business objectives. We look forward to continuing to engage with Government and industry to shape practical, forward looking policy settings that protect our digital economy, foster innovation, and ensure Australia remains a trusted and influential cyber leader on the global stage.

infotrust

SECURE YOUR FUTURE.

About Infotrust

Infotrust is Australia's leading Managed Cyber Security Service Provider. With our team of highly skilled and experienced security experts, Infotrust provides unparalleled protection to safeguard your digital assets. Our cyber consultants have a deep understanding of the unique threats faced by Australian businesses and are adept at devising robust security strategies with a specific focus of Offensive Security, Governance, Risk and Compliance, and Managed Detection and Response. Infotrust's world-leading Australian Security Operations Centre operates 24/7 to provide continuous monitoring, threat detection and incident response.

[redacted]