Horizon 2

2023-2030 Australian Cyber Security Strategy

Submission

September 2025

THALES
Building a future we can all trust

Foreword

We are pleased to enclose Thales Australia's submission to developing Horizon 2 of the *2023-2030 Australian Cyber Security Strategy*.

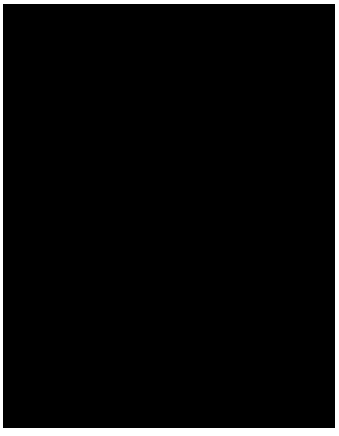
The need to accelerate our national cyber resilience has become more pronounced since Horizon 1. Thales Australia supports capabilities across the land, sea, air, space and digital domains and we have seen the cyber threat intensify in distinct ways. Industry reporting suggests Australian ranks fourth globally for cyber threats to our Critical Infrastructure;[i] the frequency and size of data breaches still impact vast swathes of our society. At the same time, it has never been more important for a national approach to cyber security to underwrite our nation's productivity, prosperity, economic security, and sovereignty. Cyber security enables a dynamic and resilient Australian economy to fully harness data and digital technology, and both develops and protects our skilled and adaptable workforce.

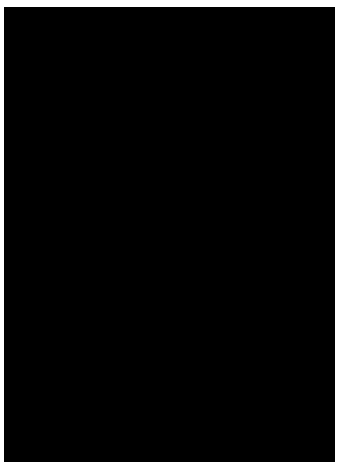
The rapid deployment of generative and agentic AI has been a defining feature of technological and economic development in Horizon 1; the Department of Industry, Science and Resources projects for example that AI and automation could contribute up to AU$600 billion annually to Australia's GDP by 2030.[ii] However, as Australia's Privacy Commissioner notes,[iii] the productivity dividends from AI cannot be realized without the trust and confidence of the Australian public.

Thales Australia is a uniquely sovereign Defence and Technology company – we trace our history supporting critical Defence capabilities in Australia for over 100 years. Today, our national contributions range from stewarding Australian defence manufacturing capabilities to providing defence-grade cybersecurity to Government, Critical Infrastructure and Enterprise customers that support Australian society and our democratic way of life. We 'walk the talk' with cyber security through our lived experience as both a Critical Infrastructure operator and a Prime within the Defence Industry Security Program.

Our submission provides our unique perspective that fuses our experience as a national provider of cyber products and services, an operator of critical infrastructure assets, a highly regulated entity, and a Defence and Technology company with a national security and engineering DNA. We offer actionable recommendations mapped to the Horizon 2 Shields based on both our lived experience supporting the security of our clients, our enterprise and our supply chain.

We commend the Commonwealth's consultative efforts to develop Horizon 2 and look forward to continuing our support to informing and operationalising our cyber resilience.





Summary of Recommendations

Shield One: Strong businesses and citizens

Targeted CI cyber awareness

1. Government cohere and further develops cyber awareness messaging to CI operators under a single brand and hub. Messaging should focus on critical data protection and consolidates role-based sector packs and checklists.

Shield Two: Safe Technology

Secure-by-Design at the Edge

2. Government considers CIRMP rule amendments to require risk-based vulnerability management in OT and edge devices to enhance critical data security. These amendments can include requirements for zero-trust access, integrity controls and transfer logging for designated critical datasets, and supplier FOCI attestation.

3. Additional regulation for designated critical datasets be considered to standardise dataflow and logging fields, require dataset registers and provenance records, mandate logging and risk-assessments of cross-border transfers. Supporting measures could include annual transparency reporting to a standard template; and the application of limited-use safe harbour for timely disclosure.

4. Vendor-transparency rules for edge/OT and critical-data service suppliers are developed by Government to require disclosure of beneficial ownership and control, foreign-government ties, offshore support locations and data-access pathways. Supporting measures could include reasonable notification of material changes; a vulnerability disclosure policy, and a Software Bill of Materials (SBOM) on request. These rules should be made enforceable through regulator audit powers, penalties and procurement ineligibility until remedied.

5. Government considers procurement levers (such as the Commonwealth Procurement Rules) to operationalise edge and critical data security rules, including e.g. a requirement for suppliers to share OT security information with government buyers, and accept a standard right to audit.

Responsible AI and Emerging Technology Controls

6. Government develops responsible use of AI rules and regulates custodians of designated critical datasets, such as large AI service providers and Commonwealth entities, to e.g. require data classification before use, disclosure of processing and storage locations and reporting of AI-related breaches.

7. Government to develop and promulgate sector-specific notes on AI in OT that sets guardrails for data location, retention and training settings; defines supplier transparency and compensating controls (aligned to recognised OT security standards).

8. Government considers procurement levers to incentivise AI security, including the mandating of model clauses (such as 'no-training' warranties, data-location disclosure, prompt/output logging, incident cooperation and model-change notification), and applying procurement ineligibility for non-compliance.

Shield Three: World Class Threat Sharing and Blocking

Scaling national threat sharing

9. Government regulates mandatory participation in the whole-of-economy threat intelligence sharing network as an additional Positive Security Obligation (PSO) that apply to all CI owners and operators.

10. Mandatory participation reforms be accompanied by the appropriate scaling of ASD's existing Cyber Threat Intelligence Sharing platform, the government's threat sharing acceleration fund, including leading, seeding and participating in sectoral ISAC initiatives where appropriate.

11. The link between the whole-of-economy threat intelligence network and scaled national threat blocking capabilities be co-designed and articulated to participants in both initiatives, including through the Executive Cyber Council, with the view on unlocking strategic complementarity and operational intelligence synergies.

12. The Executive Cyber Council be given an accountable leadership role in championing and driving public-private collaboration to implement, drive uptake, de-risk and operationalise whole-of-economy threat intelligence sharing and blocking; this should include demonstrable measures of success.

13. The de-risking of whole-of-economy threat sharing implementation is not conducted through more 'pilots', but through deliberate rollout and iteration. Implementation should bias for action, incorporate collaborative co-design, and public-private leadership and steering (including through the ECC). Protective capabilities should also be enhanced for the increase in sharing platforms and participants.

Blocking threats at national scale

14. Government enhances and accelerates Horizon 2 threat blocking initiatives into a national scale program, cohering and operationalising whole-of-economy intelligence sharing for cyber security and scams prevention.

15. Government develops grant programs for SMEs to seed and support organisational Security Operations, creating a 'bottom up' effect to complement a national 'top down' approach to threat blocking.

Exercising Cyber Conflict and Crisis response

16. Government enhances, and co-designs with CI stakeholders, cyber conflict and crisis mechanisms that acquits ASIO's latest threat assessment, including accounting for multi-domain 'threat convergence' and 'high-impact sabotage'.

17. Cyber conflict and crisis scenarios include 'analogue bypass' scenario exercises where CI/[redacted] operators are exercised on non-digital and non-networked mechanisms to sustain critical operations during severe disruptions to digital connectivity.

18. Public/private cyber conflict preparedness exercises that are appropriately cross-walked with the National Defence Strategy and relevant ADF Contingency plans, and involves Defence, and relevant CI and Defence Industrial Base stakeholders.

19. Government-led national awareness-raising initiatives and campaigns for both businesses and society on 'what to do' during cyber conflict or crisis.

Shield Four: Protecting Critical Infrastructure

Systemic technical debt remediation

20. Government conducts specific analysis to assess the extent of technical debt in select sectors, including energy, telecommunications and data storage and processing. This analysis should also identify the estimated costs of remediation

and uplift to meet security standards and anticipated requirements from autonomy, AI and Post-Quantum Cryptography (PQC).

21. Government considers the development of public/private financial mechanisms that support sovereign capital investment in CI technical debt remediation and uplift. These mechanisms should be informed by the above analysis and strategic security outcomes which include addressing FOCI risks or concerns.

Dependency management

22. Government commissions a program of work to map critical interdependencies and nodes within the CI estate to identify shared assets or systems held in common where risk management ownership is not clear. This work should also identify collections of devices/systems that are not individually owned or operated as a single entity but collectively form a critical infrastructure asset or eco-system. Cross-sectoral cyber exercises can be a useful way of validating dependency mapping.

23. Where multiple CI entities use or transact an asset or system, Government should also articulate appropriate risk management approaches.

24. To mitigate against prolonged or systemic outages, Government should consider and determine service level agreements between CI operator that is informed by validated dependency mapping work.

25. Sector-specific Risk Management Plan requirements (such as the TSRMP) are developed further to reduce regulatory duplication and drive better specificity in risk management, which accounts for commonly operated assets.

OT Resilience

26. Government considers regulation and/or mechanisms to require and incentivise for large construction firms to adhere to OT build requirements to drive accountability across consortia and supply chains.

27. Government considers the establishment of a CI supplier panel for infrastructure builds that considers adherence to relevant security framework and maturity standards, trusted supply chains for componentry (which can also e.g. generate required OT system logging).

Supply Chain Risks

28. Government identifies and map critical component dependencies across CI sectors and engage with key manufacturers to ensure Australian prioritisation for ongoing supply. This will requires foreign policy and trade considerations to support productive relationships with key nations and suppliers.

Shield Five: Sovereign Capabilities

Sovereign CI and OT Testing Facilities

29. Government considers regulating national and industry holdings of critical components and materials to ensure continuity of critical operations and services during sustained outages in the event of crisis or conflict.

30. Government develops or commission sovereign testing labs and facilities so that critical components can tested against vulnerabilities, enhancing CI and government decision making on component selection.

Active Cyber Defence

31. Government provides legal and regulatory clarity on industry active cyber defence activities (including lawful disruption) to encourage and enhance the ability for the whole-of-economy to mitigate and respond to malicious cyber activity.

32. Government develops clear mechanisms to support public/private collaboration on lawful cyber disruption activities. This could include specialised panel arrangements with sovereign cyber providers to scale government's ability and capacity to respond.

Shield Six: Strong region and global Leadership

Regional Engagement

33. Government implements a 'white-label' requirement for industry contracted to provide cybersecurity support and services on behalf of the Commonwealth in the region, where only the Australian Government brand is used in service delivery.

34. As the Commonwealth efforts to support our region scales in Horizon 2 in terms of tempo and complexity, Government invests in additional measures to increase the numbers, seniority and technical abilities of Australian Government officials conducting and managing complex cyber programs and industry consortiums.

Shield 1
Strong businesses and citizens

Targeted CI cyber awareness

1. Government has undertaken a significant amount of work in Horizon 1 on both expanding national cyber security awareness, including the commendable 2024 release of the Act Now and Stay Secure campaign. However, large-scale data breaches still impact many areas of the Australian economy and society; recent trends in the Office of the Australian Information Commissioner's (OAIC) Notifiable Data Breaches Report still suggest data breaches from cyber security incidents are increasing year-on-year.

2. Critical Infrastructure (CI) operators are in a challenging position with data protection. They are custodians of nationally significant datasets but typically have complex supply chains and/or Operational Technology (OT) environments that can create opaque data pathways and environments. CI operators should be prioritised for targeted awareness and guidance, with a focus on challenging issues such as data handling for Operational Technology (OT), Internet of Things (IoT) and Industrial Internet of Things (IIoT), supplier provenance and transparency.

3. General awareness campaigns often lack the ability to drive specific behaviours needed to protect IoT and OT data flows and critical datasets. CI operators typically face safety constraints and narrow change windows and often postpone remediation. IoT fleets often include ageing devices with weak identity, limited patching and third-party management, which increases exposure. Guidance and terminology often vary across regulator, government agencies and vendors, which splits attention and creates rework.

4. We submit that security adoption improves when Government points to clear exemplars of 'what good looks like' for IoT and OT data protection, provides copy-ready configurations and playbooks, and requires suppliers to deliver standardised provenance and data-access transparency. The 2024 Australian Cyber Security Centre (ACSC) Principles of Operational Technology Cybersecurity is commendable guidance and can be expanded upon to include guidance on logging and architecting. As many OT estates are principally composed of Original Equipment Manufacturer (OEM) equipment with build commonalities within sectors, Government should consider more specific guidance on logging outcomes for common assets and devices.

Recommendation

5. Government cohere and further develop cyber awareness messaging to CI operators under a single brand and hub. Messaging should focus on critical data protection and consolidates role-based sector packs and checklists.


Shield 2
Safe technology

Secure-by-design at the edge

6. Australians are living through dynamic technological change that is intensifying as AI and quantum computing reshape how we live and work. This technological change is also characterised and underwritten by long-term infrastructure builds in energy and data storage and processing, for example, with multi-decade lifespans that must accommodate capabilities and risks we cannot yet fully predict. Software changes quickly; Industrial Control Systems (ICS) and OT do not. Poor design choices made now will lock in technical debt for decades.

7. Zero trust offers a practical path but is hardest at the edge. Long-lived OT, ICS and consumer energy resources operate in locations that may be remote, hazardous or both, and were not built for persistent connectivity. Operators rely on remote access, which requires strong identity, segmentation and continuous verification.

8. Supplier concentration and opaque remote access compounds risk. Many providers are foreign-owned and service Australian assets from multiple jurisdictions. Some edge devices include undisclosed latent capabilities e.g. embedded cellular connectivity, creating unmanaged access paths.

9. Current regulation, including the *Security of Critical Infrastructure Act* (2018) (SOCI), already provides a pathway to establish a single, risk-based model that applies zero trust at the edge and protects critical data through an expansion of the existing CIRMP Rules. Those Rules can be enhanced to introduce a national risk matrix for edge and OT assets with retrofit control profiles, require an exception register for non-conformant assets, and set supply-chain assurance duties that include FOCI attestation and transparency.

10. Regulatory enhancements can also include co-governance with industry (especially responsible custodians of designated critical datasets) on a national access and data-flow schema and a secure reporting gateway with safe-harbour protections. Together, these enable lawful sharing, a common taxonomy and faster remediation as well as better risk management and dependency identification across sectors.

11. This schema can include prescriptive guidance on least-privilege access with continuous verification, log access and inter-jurisdictional transfers, preservation of independent backups or images for retrospective assurance, and requirements for a dataset register, provenance records and tamper-evident logs, including records of broker and sub-processor use. To support audit and interoperability, the model could align to IEC 62443 for OT, NIST SP 800-207 for zero trust, and AS ISO/IEC 27001 and 27002. Finally, Government should consider procurement levers, such as updates to the Commonwealth Procurement Rules, to operationalise these requirements in government buying decisions.

Recommendations

12. Government considers CIRMP rule amendments to require risk-based vulnerability management in OT and edge devices to enhance critical data security. These amendments can include requirements for zero-trust access, integrity controls and transfer logging for designated critical datasets, and supplier FOCI attestation.

13. Additional regulation for designated critical datasets be considered to standardise dataflow and logging fields, require dataset registers and provenance records, mandate logging and risk-assessments of cross-border transfers. Supporting measures could include annual transparency reporting to a standard template; and limited-use safe harbour for timely disclosure.

14. Vendor-transparency rules for edge/OT and critical-data service suppliers are developed by Government to require disclosure of beneficial ownership and control, foreign-government ties, offshore support locations and data-access pathways. Supporting measures could include reasonable notification of material changes; a vulnerability disclosure policy, and a Software Bill of Materials (SBOM) on request. These rules should be made enforceable through regulator audit powers, penalties and procurement ineligibility until remedied.

15. Government considers procurement levers (such as the Commonwealth Procurement Rules) to operationalise edge and critical data security rules, including e.g. a requirement for suppliers to share OT security information with government buyers, and accept a standard right to audit.

Responsible AI and Emerging Technology Controls

16. Untracked data leakage from AI use poses a significant data and privacy risk. There is a live human-error risk where staff paste sensitive content into external tools without controls, logs or contractual limits on retention or model training. Bot-to-bot interactions can create shadow datasets and trigger unsanctioned polling.

17. Opaque AI data access compounds the risk. Organisations cannot effectively observe or track cross-border data transfers, downstream reuse for model improvement, or who accessed what and why. Many AI models or providers do not recognise sector-specific national security impacts, including exposure of critical datasets and operational telemetry. Similar data-handling risks arise from advanced IoT at the edge, 5G exposure patterns and quantum capabilities.

18. Our contemporary controls do not match these vulnerabilities. Some AI providers retain prompts and outputs by default unless contracts or settings disable it and may process data offshore. Plugin and broker ecosystems can forward data to third parties without notice. CI operators face added risk if OT data, network maps or maintenance records enter AI tools. Supplier transparency on ownership, control, hosting and data-access paths for AI tools is inconsistent. Reporting of AI-related exposure is uneven and discouraged without clear safe-harbour settings and practical guidance.

19. Current regulation such as the *Cyber Security Act 2024 (Cth)* provides levers to set a national baseline for AI data handling as well as standardising of logging and reporting schemas. This would enable limited-use safe harbour for timely disclosure through a designated secure gateway. For CI there is existing regulation that can enable embedded obligations to allow responsible entities assess and control AI risks to OT and designated critical datasets.

20. Government should consider AI security guidance cohered as a ready-to-use implementation package, which can include an acceptable-use policy, a vendor due-diligence checklist, contract clauses on non-retention and training, and logging patterns for common platforms, a standard dataflow and prompt-logging schema, sample red-team tests and model risk-register templates.

21. Government procurement is also another lever to help reinforce baseline AI security across different supply chains. This can include requirements aligned to the Technology Vendor Review Framework, and Foreign Ownership, Control or Influence (FOCI) guidance on data-location disclosure, incident cooperation and change notifications.

Recommendations

22. Government develops responsible use of AI rules and regulates custodians of designated critical datasets, such as large AI service providers and Commonwealth entities to e.g. require data classification before use, disclosure of processing and storage locations. and reporting of AI-related breaches.

23. Government to develop and promulgate sector-specific notes on AI in OT that sets guardrails for data location, retention and training settings; defines supplier transparency and compensating controls (aligned to recognised OT security standards).

24. Government considers procurement levers to incentivise AI security, including the mandating of model clauses (such as ‘no-training’ warranties, data-location disclosure, prompt/output logging, incident cooperation and model-change notification), and applying procurement ineligibility for non-compliance.


Shield 3
World-class threat sharing and blocking

Scaling national threat sharing

25. We commend Government's initiatives to create a whole-of-economy threat intelligence network in Horizon 1, including Executive Cyber Council public-private collaboration, the enhancement of ASD's Cyber Threat Intelligence Sharing (CTIS) platform, and the launch of a threat sharing acceleration fund. These important activities set up sustainable foundations, including lessons learnt, that enable threat sharing to scale to support the whole-of-economy.

26. In Horizon 2, we call on Government to scale threat intelligence sharing rapidly and extensively so that allow us to keep pace nationally with intensifying threats (that are increasingly AI-enabled). Simply put, we need to scale national threat sharing at the pace of the threat, accelerating whole-of-economy participation and benefits.

27. Cyber threat intelligence sharing is currently practiced by comparatively few and relatively mature organisations that have made proactive investments in operationalising threat intelligence for cyber security. Participation in threat sharing is largely voluntary and skewed towards larger organisations, with many parts of our economy simply not resourced to do so – smaller and less mature sectors are often underrepresented but may bear the biggest impacts from not being cyber intelligence enabled.

28. As a result, our national situational awareness is incomplete and arguably mis-represented simply because only larger and mature organisations are contributing to threat sharing, with blind spots and vulnerabilities in less-resourced and arguably more vulnerable sectors. A notable exception is in Federal Government where there has been 2024 Protective Security Policy Framework direction requiring all Australian Government entities to enrol in ASD's CTIS platform – a direction that we commend.

29. Although it is important to increase threat sharing participation to increase the volume of CTI being shared, it is only with the right contextualisation can participants effectively operationalise threat intelligence to protect their attack surface, and their sector's. Without the right frameworks, resources, tools and techniques to support contextualisation, participants will not be able to get the right 'signal from the noise', and threat intelligence will likely be counter-productive to an already-busy security team.

30. Threat sharing participants must be enabled from the outset to effectively consume, operationalise and then share intelligence to genuinely enable participation and the benefits from CTI sharing – for the individual organisation, sector, and to support national objectives. Again, we commend the Government's efforts to develop a Health Cyber Sharing Network and submit that this Pilot must be scaled out to our CI sectors as soon as practicable – we cannot let 'perfect be the enemy of good'.

31. Importantly, a whole-of-economy threat intelligence network is only useful to the vast majority of society if that intelligence can be operationalised to support threat blocking at-scale, protecting small-medium enterprises and individuals. Although threat blocking mechanisms and activities have been developed in Horizon 1 initiatives, we submit that these activities must be accelerated and scaled to both keep pace with threats and operationalise and derive dividends from our collective investments in threat-intelligence sharing. How CTI sharing can enable better threat blocking (including for scams) should be co-designed and clarified. Clarity and consultation can help remove FUD (Fear Uncertainty Doubt) about how shared CTI is used, can enable more targeted and curated CTI sharing, and create an effective sharing and blocking ecosystem. In simplistic terms, if cyber security at scale requires machines to mitigate (adversary) machines, then we need to inform and tune our machines correctly and consistently.

32. Finally, scaling out threat sharing also naturally increases the attack surface of sharing platforms and participants, including cyber, personnel and FIS interest and risks. Effective scaling of whole-of-economy threat sharing must also be enabled and underwritten with additional capabilities and capacity to protect an increased number of platforms and participants.

Policy considerations

33. To accelerate and scale whole-of-economy threat intelligence, Government must consider regulation to compel participation by those that have the means to do so. We submit that the current CI/[redacted] reform already provide a widely accepted mechanism to define those that have the means and requirements to participate in intelligence-sharing, even if it is just to 'consume' to start. The prescriptive *actionable scam intelligence* obligations for regulated sectors and

designated businesses under the *Scams Prevention Framework Act 2025* is also instructive.

34. If threat-intelligence sharing is not mandated through regulation, we submit that strategic objectives for the whole-of-economy threat intelligence network will not be met. There simply will be not be sufficient critical mass to operationalise whole-of-economy objectives: there will be 'blind spots' preventing a true national/sectoral intelligence picture given the currently skewed participation by mature volunteers, real time threat sharing will only benefit those with the means and willingness to share, which may undermine confidence in this critical initiative by those that are 'excluded'.

35. By enabling those with the means to share (typically large organisations with mature cybersecurity) to benefit from near real-time threat intelligence, we are effectively 'shaping' threat actors to target sectors and organisations who have not had the benefit of operationalising near real-time intelligence. Put another way, if we maintain the status quo of voluntary opt-in to ASD's CTIS platform and other threat sharing mechanisms, we may be increasing the likelihood and impact of cyber breaches on those requiring the most protection.

36. Regulatory compliance must be supported by mechanisms and incentives to operationalise CTI sharing, with a deliberate focus on uplifting CI sectors least able to threat-share. CTI only works for organisations if it is additive, and not distractive. This requires changing paradigms quickly on intelligence/risk-led approaches to cybersecurity (as opposed to mere compliance and 'ticking the box'). Operationalising CTI naturally requires sector-specific contextualisation and enablement such as ingestion rules to distil 'signal from noise' – there is no 'one size fits all'.

37. Sector-specific sharing mechanisms such as Information Sharing and Analysis Centres (ISACs) are critical in operationalisation, but Government has a role in leading, actively participating and/or seeding these initiatives to ensure and or promote alignment with strategic policy objectives, including with ASD's CTIS platform, inclusivity and not-dominated by large mature participants, capability uplift and education on 'why intelligence' as opposed to what can often be a largely technical discussion on CTI formats and rules.

38. Government has already commendably commenced this work with the threat-sharing acceleration fund and the Health Cyber Sharing Network pilot, including key lessons learnt. These mechanisms must be scaled and phased in line with any

proposed regulation on threat-sharing. To keep the status quo of threat-sharing as a voluntary activity for CI entities, progressing at the rate of 'Pilot' programs with limited enablement is to not be realistic in the face of the scale and speed of national cyber threats. We must avoid the perfect being the enemy of the good, and rolling out more Pilot programs that effectively 'kicks the can down the road'.

39. The strategic imperative and endstate must be the uplift of relevant whole-of-economy participants to be able to use CTI to combat threats quickly and cover our national attack surface holistically. If regulation is not introduced to mandate CI threat sharing (with the right sectoral enablement and operationalisation), we will perpetuate a situation where:

- only large and mature organisations benefit from threat sharing, and threat actors are 'shaped' to target those without the means to threat-share (i.e. the more vulnerable)
- less mature sectors are inadvertently systemically weakened (being less 'covered' by default)
- industry resentment may be created around threat-sharing due to de-facto exclusion (making future uptake more difficult), and
- there are critical gaps in the national intelligence picture due to the lack of critical mass and the skewed nature of participation.

Recommendations

40. Government regulates mandatory participation in the whole-of-economy threat intelligence sharing network as an additional Positive Security Obligation (PSO) that apply to all CI owners and operators.

- This regulatory reform can be phased with mandatory participation first applying to Enhanced Cyber Security Obligations (ECSOs) applicable to [redacted] before broader participation by PSO holders.

41. Mandatory participation reforms be accompanied by the appropriate scaling of ASD's existing Cyber Threat Intelligence Sharing platform, the government's threat sharing acceleration fund, including leading, seeding and participating in sectoral ISAC initiatives where appropriate.

42. The link between the whole-of-economy threat intelligence network and scaled national threat blocking capabilities be co-designed and articulated to participants in both initiatives, including through the Executive Cyber Council, with the view on unlocking strategic complementarity and operational intelligence synergies.

43. The Executive Cyber Council be given an accountable leadership role in championing and driving public-private collaboration to implement, drive uptake, de-risk and operationalise whole-of-economy threat intelligence sharing and blocking; this should include demonstrable measures of success.

44. The de-risking of whole-of-economy threat sharing implementation is not conducted through more 'pilots', but through deliberate rollout and iteration. Implementation should bias for action, incorporate collaborative co-design, and public-private leadership and steering (including through the ECC). Protective capabilities should also be enhanced for the increase in sharing platforms and participants.

Blocking threats at national scale

45. We commend Government's efforts to develop threat blocking at scale, including through the National Cyber Intel Partnership (NCIP) Threat Blocking Scheme. As we submitted above, these activities must be accelerated and scaled to both keep pace with threats and operationalise and derive dividends from our collective investments in threat-intelligence sharing.

46. The indiscriminate and opportunistic nature of cybercrime often means our most vulnerable and powerless are at risk, such as scams targeting small businesses, our elderly and our young. We commend also the work of the National Anti-Scam Centre in its whole-of-economy efforts create public/private partnerships to collaborate and disrupt scams. The threat blocking/sharing intersection point

with the *Scams Prevention Framework Act 2025* (SPF) provides drivers and opportunities to operationalise this at scale.

47. As many of our national cyber threats are already enabled by AI and high-performance compute, so should our national shields. We have recommended earlier a fundamental requirement for CI to be regulated to threat-share; for organisation/sectoral protection and to provide the 'critical mass' enabling national-scale blocking activities. Together with SPF actionable scam intelligence obligations, Australia can be a world-leader in operationalising our own unique 'secret sauce' CTI to block at national scale. We can keep pace and move ahead of dynamic threats through leveraging both generative and agentic AI to support threat analysis, detection and prediction – a 'national detection engine'. Quicker and more reliable detection can enable blocking at the speed of adversary 'attack cycles', enhancing our national cyber common operating picture, and supporting quicker, targeted and scaled disruption efforts e.g. to enable government agencies to better 'hack the hacker'.

48. There are of course numerous considerations and challenges to operationalise threat blocking at national scale. The sovereignty and security of national level 'big data' sets are critical due to both the 'attractiveness' as a target for adversaries, and privacy expectations and obligations on how citizen data is handled. These sovereignty and security requirements apply to hosting, transmission and handling, including how AI tools are selected, curated and managed to operationalise intelligence. Big data compute costs are costly, but the 'narrow and deep' type of analysis may be a suitable candidate for utility-scale quantum computing, enabling the Australian Government to unlock synergies in its recent strategic investments in this sector.[iv]

49. A calculated benefit in designing and executing threat blocking at national scale is the requirement for and subsequent investment in Australian innovations to overcome novel challenges in achieving this strategic vision. These innovations will likely become candidates for commercial export, which we submit is a fundamental requirement for our national ambition in becoming a world leader in cyber by 2030. Australia has had a proud recent history of creating global technology leaders; we have the right conditions to create globally significant cyber champions as well. Although national cyber innovation is deserving of comprehensive separate consideration, our position here is that national-scale CTI sharing and blocking endeavours will have the benefit of requiring sovereign commercial innovation that benefits many aspects of our economy, society and international standing.

50. Blocking threats at scale is not only 'top-down' – Government should also invest in how operationalising national CTI can be executed from 'bottom up'. We have recommended above the requirement for further government investments in ISACs and sharing acceleration. However, for the average SME, threat sharing may not be a realistic proposition. This does not mean they can only rely on their Managed Services Providers (MSP) to block threats and be without agency in a national CTI ecosystem. Government should consider SME grants to adopt Security Operations functionality across their environments for SMEs to at least be able to ingest CTI proactively. As well as democratising CTI (which can often be opaque and simply 'vendor speak' to most), it also helps 'bake-in' intelligence-led cyber defence practices for SMEs as they grow into larger national enterprises; in other words, 'start them young' with grants and guidance, knowing that we are helping secure our future national champions.

51. Finally, we recognise that these are ambitious and challenging concepts we have submitted above. Blocking threats at national scale requires an effective crosswalk for all 6 shields in the 2023-2030 Australian Cyber Security Strategy – a 'national shield' in layperson speak. However, we submit that these national intelligence sharing + blocking initiatives, more than most, are the critical asymmetric mechanisms that will enable Australia to become 'the most cyber secure country in the world by 2030'. In the face of our exponentially increasing attack surfaces, sustained threat dynamism and sophistication, and geostrategic instability, we must execute boldly at scale and speed, combatting the malicious use of technology with the smart and beneficial use of technology. Our national ambitions here must be met with step-change, and not small iterative measures.

Recommendations

52. Government enhances and accelerates Horizon 2 threat blocking initiatives into a national scale program, cohering and operationalising whole-of-economy intelligence sharing for cyber security and scams prevention.

53. Government develops grant programs for SMEs to seed and support organisational Security Operations, creating a 'bottom up' effect to complement a national 'top down' approach to threat blocking.

Exercising Cyber Conflict and Crisis response

54. Government has implemented significant bodies of work to e.g. activate ECSOs (including cyber exercise) and map all-hazards consequence management to crisis response arrangements. ASD's long-running National Exercise Program helps operationalise these arrangements. These efforts have been both critical and commendable in creating foundations for our national cyber resilience.

55. However, as the Director General of Security notes in the most recent ASIO Annual Threat Assessment, threats have converged in an unprecedented way, with the security environment significantly degraded, and 'high-impact sabotage' specifically called out. The current regime of cyber conflict and crisis preparedness is arguably not commensurate to the current threat assessment.

56. Cyber conflict and crisis preparedness activities must be scaled out to exercise response against targeted sabotage events and likely systemic impacts. Government must lead transparently in exercising worst-case scenarios with CI/[redacted] operators, such as 'analogue bypass' type scenarios where non-digital, non-networked methods are used to sustain critical government and societal type operations, communications and decision making.

57. This may require a sobering examination of offline and physical alternatives to digital means to preserve continuity and control during severe disruptions to digital connectivity. These examinations and exercises will practically differ by sector and should rightly include factors such as non-digital communications (e.g. landline and radios), physical controls for OT/ICS, and manual processes for logs, checklists and reference physical signatures for certain systems. These exercises will naturally highlight deficiencies in skills such as in manual/analogue procedures, and even security clearances for key personnel, given the national security implications and collaborative requirements of these scenarios.

58. Importantly, to genuinely prepare for conflict, these preparedness activities with CI/[redacted] operators must be cross-walked with Australian Defence Force contingency planning during conflict type scenario: Critical Infrastructure continuity should not only be framed only as important to preserve societal operations and services, it is a critical ADF dependency for force projection, force preparedness, statecraft, allied interoperability, the Defence of Australia,

and our national support base for long-term campaigning and deterrence – the 'pointy end' of how we preserve our democratic way of life during conflict.

59. These are not unprecedent concepts; there are plenty of lessons learnt from Ukraine's multi-year defensive campaign against Russian aggression. Australia's adversaries are sophisticated and will be incentivised to target our whole-of-economy 'soft underbelly' to disaggregate and dislocate our ability to defend ourselves. Key targets for adversaries will not be limited to 'hard' targets like energy supply; the disruption of key societal functions such as banking and retail may go some way in undermining the political will for Australia to for example, remain in an allied military coalition in the Indo-Pacific.

60. It is perhaps revealing that in the Horizon 2 Policy Discussion paper that Defence or the ADF is not mentioned once. We submit that significant work needs to be done with CI and industry to enable a public/private crosswalk of Horizon 2 strategies and initiatives with the National Defence Strategy, including the fundamental dependencies between CI/[redacted] resilience and preparedness to conflict response and deterrence.

61. Although significant work may be ongoing in the non-public and security-classified domains, this is arguably ineffective if largely behind closed doors. CI operators and industry must be engaged regularly on genuine cyber conflict-type exercise scenarios that educates industry leaders, articulate inter-dependencies and highlight potential deficiencies in how CI enables the broader ADF National Support Base.

62. Remediating deficiencies, which may include building contingency supply capabilities and 'analogue bypass' type mechanisms, may be costly, but we submit should be appropriately built into broader consumer prices and the cost of doing business in a geostrategically dynamic world. To strategically prepare for cyber conflict requires commensurate market changes that incentivise CI operators to design and operate for efficacy (i.e. resilience and redundancy) and not just cost efficiencies. Government has a role to responsibly lead and steward changes in these market dynamics in the face of heightened conflict risks – this is not something that can be left to industry to develop in isolation; it simply won't happen without government leadership.

63. Government also has a leadership role in explaining the importance of cyber conflict preparedness and exercises to the public in a calm and consistent manner. This can be difficult and sensitive, but is not novel – Sweden, Norway

and Finland for example in late 2024 launched public campaigns advising their citizens what to do in the event of an invasion. Systematically raising public awareness of what to do in a conflict is not 'warmongering' – it is being realistic about the geostrategic environment and arguably a fundamental step in building societal resilience that matches the repeated Government assessments on the unprecedented nature of our deteriorating threat environment.

Recommendations

64. Government enhances, and co-designs with CI stakeholders, cyber conflict and crisis mechanisms that acquits ASIO's latest threat assessment, including accounting for multi-domain 'threat convergence' and 'high-impact sabotage'.

65. Cyber conflict and crisis scenarios include 'analogue bypass' scenario exercises where CI/[redacted] operators are exercised on non-digital and non-networked mechanisms to sustain critical operations during severe disruptions to digital connectivity.

66. Public/private cyber conflict preparedness exercises that are appropriately cross walked with the National Defence Strategy and relevant ADF Contingency plans, and involves Defence, and relevant CI and Defence Industrial Base stakeholders.

67. Government-led national awareness-raising initiatives and campaigns for both businesses and society on 'what to do' during cyber conflict or crisis.

Shield 4

Protected critical infrastructure

Systemic technical debt remediation

68. Artificial intelligence and automation will power the productivity step-change the Australian workforce needs to remain competitive and drive our economy, but these technologies are reliant on energy, data, telecommunications and secured OT components. The technology debt held in the energy, data processing and storage and telecommunications sectors is considerable and needs to be quantified and subsidized by Government to support the scale of remediation required.

69. Our current national infrastructure may not be adequate for current demand let alone the rapidly increasing needs of transformative technologies such as automation, AI and also Post-Quantum Cryptography (PQC) security data processing and storage sector operators have expressed private views that the sector is at serious risk of sustained outage if significant demand hits all centres simultaneously, such as the release of popular video games coinciding with peak usage periods.

- The cost of remediating CI technical debt and resilient uplift across the whole-of-economy is difficult to quantify, but likely to run into significant billions. We provide some examples from telecommunications, utilities and data storage and processing sectors:

- Costs of transitioning from legacy infrastructures (copper) in fibre to the node and hybrid fibre coaxial networks in the telecommunications sector is estimated at A$10-15 billion.

- The Australian Energy Market Operator's (AEMO) Integrated System Plan (ISP) projects $12.7 billion in transmission investment by 2050, much of which addresses legacy constraints.

- Our own experience in the data and processing sector suggests that approximately 0.5% of asset Total Cost of Ownership (TCO) investment may be required by entities to uplift to current requirements; a similar amount may further be required to account for growing need. An expectation of the same again (at least) may be required to achieve suitable functionality.

70. Government has a role in both calling out systemic technical debt as a critical vulnerability in our national CI security, and leading strategic public/private mechanisms to address this urgently. This is both to support CI security that underpins the resilient operations of many parts of our economy and the significant national productivity dividends with autonomy and AI. In addition to quantifying the challenges, Government must also provide clarity and decisiveness on the role of private capital in remediating CI technical debt, especially as it relates to Foreign Ownership Control and Influence (FOCI) risks in a degraded security and geopolitical environment.

Recommendations

71. Government conducts specific analysis to assess the extent of technical debt in select sectors, including energy, telecommunications and data storage and processing. This analysis should also identify the estimated costs of remediation and uplift to meet security standards and anticipated requirements from autonomy, AI and PQC.

72. Government considers the development of public/private financial mechanisms that support sovereign capital investment in CI technical debt remediation and uplift. These mechanisms should be informed by the above analysis and strategic security outcomes which include addressing FOCI risks or concerns.

Dependency management

73. The Security of Critical Infrastructure Act (SOCI) and CI/[redacted] reforms has effectively driven entity-level risk management and raised awareness of critical dependencies at the asset and entity level. This arguably 'generalist' approach has been effective in establishing baseline security standards but more sector-specific obligations, such as risk management plans, are now required. We submit that there is a need to clearly map and manage the complexity of inter and intra sector dependencies to support holistic national resilience.

74. A consistent issue for CI entities is the complexity in defining the 'asset' where infrastructure is shared or operated by third parties. This is especially marked in the energy and telecommunications sectors where key parts of the critical asset infrastructure are commonly held and/or operated and owned by different entities which muddies the risk picture. Holistic CI risk management is often a collective endeavour which cannot be easily led or owned by industry due to both competition concerns and limited visibility of the entire sector's infrastructure 'estate'.

75. For example, the risk management of shared estate or infrastructure, "nodes" and/or edge devices that may have a collective (aggregated) impact that is greater than the individual asset or device is problematic. As these elements of the digital infrastructure estate are held in common and/or are often not individually "owned" by a single entity, it is difficult for any single operator to understand, map or effectively own the risk management of these elements.

76. The risk management of collective or commonly held assets must be understood and managed by a central party and likely the regulator. This effort may require a significant program of discovery and analysis and might create a third asset or system type that reflects common or collective dependencies.

Recommendations

77. Government commissions a program of work to map critical interdependencies and nodes within the CI estate to identify shared assets or systems held in common where risk management ownership is not clear. This work should also identify collections of devices/systems that are not individually owned or operated as a single entity but collectively form a critical infrastructure asset or eco-system. Cross-sectoral cyber exercises can be a useful way of validating dependency mapping.

78. Where multiple CI entities use or transact an asset or system, Government should also articulate appropriate risk management approaches.

79. To mitigate against prolonged or systemic outages, Government should consider and determine service level agreements between CI operator that is informed by validated dependency mapping work.

80. Sector-specific Risk Management Plan requirements (such as the TSRMP) are developed further to reduce regulatory duplication and drive better specificity in risk management, which accounts for commonly operated assets.

Operational Technology (OT) Resilience

81. Through CI/[redacted] reforms and Horizon 1 initiatives, Government has established a level of security maturity in the IT layer of the digital infrastructure landscape. We need to build on this work to urgently establish standards and policy supporting greater OT resilience for Australia. Significant infrastructure build, such as those in renewable energies, are either currently being built or are in planning to support our economy's uptake of AI and automation technologies. OT security standards need to be established to ensure the resiliency in infrastructure builds and avoid prohibitively expensive future technology debt remediation. In this respect, we commend Standards Australia and the Cyber and Infrastructure Security Centre's (CISC) work in officially adopting the AS IEC 62443 series as national standards for protecting OT.

82. Many large infrastructure builds are often performed through consortia that may not build to standards specified by Government which generates additional technical debt. End asset owners and operators need to be empowered with clear policies and guidance to drive consortia builders to meet standards, particularly in sectors dominated by few builders, who are often foreign-owned and not across specific Australian requirements. There is also a separate but significant issue with FOCI challenges with large consortia infrastructure builds that Government must consider in CI security policies.

83. More broadly, if Government omits to urgently regulate or direct 'future build outs', assets will be built to non-compliant specifications with vulnerabilities that are "baked in" and difficult to correct. This would be poor practice for ICT systems, let alone OT given the much longer expected lifespan and remediation cost.

Recommendations

84. Government considers regulation and/or mechanisms to require and incentivise for large construction firms to adhere to OT build requirements to drive accountability across consortia and supply chains.

85. Government considers the establishment of a CI supplier panel for infrastructure builds that considers adherence to relevant security framework and maturity standards, trusted supply chains for componentry (which can also e.g. generate required OT system logging).

Supply chain risks

86. Australia's critical digital infrastructure is characterised by a concentration of OT manufacturers and suppliers in sectors such as telecommunications, banking and financial services, as well as a small cohort of foreign-owned Industrial Control System (ICS) component and service providers.

87. As a result, sectoral resilience can often hinge on single points of failure, especially for IT outages or vulnerabilities. A limited number of suppliers also introduces redundancy risks in key sectors such as telecommunications and semi-conductors. Further, the concentration of suppliers often means opacity in product componentry – the Australian market is effectively unable to impose standards for specialised product design or manufacturing.

Recommendations

88. Government identifies and map critical component dependencies across CI sectors and engage with key manufacturers to ensure Australian prioritisation for ongoing supply. This requires foreign policy and trade considerations to support productive relationships with key nations and suppliers

Shield 5
Sovereign capabilities

Sovereign Testing Labs and Facilities

89. We articulated above in Shield 4 how a narrow supply chain for certain sectors introduces supply chain concentration risk. An associated reality and risk is that most of these specialised manufacturers are foreign-owned, with many, if not most critical componentry manufactured offshore. However, the development of a sovereign manufacturing base for OT and specialised manufacturing like lithography is very capital intensive and is a long-term endeavour.

90. A more practical course of action would be to strengthen and harden key national supplier relationships and secure prioritisation of supply. At the same time, we should increase domestic capability to manage supply issues locally, including developing a local capability to repair/recycle key components. Importantly, given the opacity with foreign componentry, Australia must develop accessible capabilities to interrogate and test components to better understand vulnerabilities.

Recommendations

91. Government considers regulating national and industry holdings of critical components and materials to ensure continuity of critical operations and services during sustained outages in the event of crisis or conflict.

35. Government develops or commission sovereign testing labs and facilities so that critical components can tested against vulnerabilities, enhancing CI and government decision making on component selection.

Active Cyber Defence

92. Government is to be commended for its proactive 'hack the hackers' stance against large scale-malicious cyber activities against Australians in Horizon 1. Combined with Government's public attribution of cyber threat actors, this sends a determined message to malicious actors and reassurance to our businesses and society that cyber attacks on us will not go unanswered, and that there are repercussions for bad actors. We encourage Government to continue this active and proactive cyber defence positioning, and scale these activities appropriately, commensurate to the escalating threat levels to our nation.

93. We submit that the cyber industry has an increasingly significant role to play in supporting our active cyber defence activities. Many active/proactive cyber activities will naturally remain the purview of government agencies only, such as those with security-classified equities requiring ministerial and/or legislative authorities. Industry is often well placed to support government's offensive type activities with e.g. CTI sharing and enrichment, dark web monitoring, and malware reverse engineering. Some public/private partnerships are already in place to support joint disruption on telecommunication and hyperscaler infrastructure.

94. What is less clear is the ability and legal clarity that enables industry specialists to support lawful disruption activities through techniques such as deception, 'honeypots', 'sinkholing', botnet takedowns and malware C2 infrastructure seizures. Clear government definitions for legal and acceptable Active Cyber Defence (ACD) activities can encourage and enhance industry's ability to lawfully respond and mitigate malicious cyber activities – both independently and in collaboration with government. We submit that without this clarity, we miss many opportunities nationally to mitigate risk, collect and share CTI, and collaborate with government. Our national resilience is less robust due to industry inaction and omission because of legal uncertainty.

95. Encouraging and enabling industry to lawfully undertake ACD type activities will also have a strategic effect of growing demand and specialist talent in this specialised field of cyber security. This talent pool is a unique sovereign capability in itself. Government agencies and law enforcement are also subject to capability and capacity limitations – they must prioritise their operational activities, and society should not expect or rely on Government to do all the 'heavy lifting'. Importantly, many offensive ACD activities do not necessarily the intelligence 'crown jewels', specialised tradecraft and high levels of security clearances that many government agencies possess – these unique and highly-limited capabilities should be reserved for our nation's most challenging cyber and intelligence problems, such as detecting and mitigating Advanced Persistent Threats (APT). Industry, with commercial tooling (that doesn't expose government equities), can often support with cybercrime response and disruption that can help scale the overall 'hack the hackers' effect. What is required is a willingness for government to collaborate further with industry on these initiatives, and legal clarity to protect all participants in these endeavours.

Recommendations

96. Government provides legal and regulatory clarity on industry active cyber defence activities (including lawful disruption) to encourage and enhance the ability for the whole-of-economy to mitigate and respond to malicious cyber activity.

97. Government develops clear mechanisms to support public/private collaboration on lawful cyber disruption activities. This could include specialised panel arrangements with sovereign cyber providers to scale government's ability and capacity to respond.

Shield 6
Resilient region and global leadership

Regional Engagement

98. We commend the Commonwealth's efforts in Horizon 1 to engage our region through programs such as the Cyber and Critical Technology Cooperation Program (CCTCP) and Cyber RAPID. We support the planned increase in incident response, threat blocking and digital infrastructure uplift in Horizon 2.

99. As these regional programs scale, so will the requirements for Australian Government officials expand in terms of representing and managing these complex programs of work. Although industry will be critical in delivering these capabilities on behalf of the Commonwealth, the Australian Government must always be the 'face' of these efforts in terms of leadership, delivery and active participation. Currently, regional cyber assistance is often provided by contracted companies (with their own associated branding) and funded/supported by the Commonwealth. We submit that this can be counterproductive in reinforcing the Australian Government's partner of choice status in the region.

100. Many forms of industry cybersecurity support to Commonwealth agencies are already 'white-labelled' where services and products are Australian Government owned and 'fronted'. Examples of this includes Open-Source Intelligence (OSINT) investigations conducted by contracted industry specialists to support National Intelligence Community (NIC) agency collection or Law Enforcement investigations – the end products are Australian Government owned and delivered in the eyes of the relevant end users.

101. Although there is value in promoting regional public/private partnerships for certain situations such as digital infrastructure investment, the current construct of multiple vendors and contractor 'brands' delivering services on behalf of the Commonwealth in the region introduces unnecessary Australian Government 'brand dilution' risks that detract from the intended geostrategic messaging and effects. This risk is exacerbated during situations if Australian Government have limited capability and/or capacity to manage in-country delivery, which can happen due to for example, staffing constraints, if officials are not sufficiently senior or experienced enough, or do not have the technical knowledge to ensure delivery quality.

102. Multiple vendor and services providers being allowed to use their individual brands may also add to a competitive industry dynamic in the region – this is often not lost on our regional government stakeholders.

103. A 'white-labelling' requirement for Australian Government contracted services should be implemented that prevents or limits individual company brands to be used (or otherwise promoted) during Commonwealth delivery of cybersecurity support in the region. This coheres the Australian Government brand and messaging in the region, clarifies for our regional stakeholders the nature of Australian Government support, and reduces unproductive competitive risk among vendors that can impact on geostrategic messaging.

Recommendations

104. Government implements a 'white-label' requirement for industry contracted to provide cybersecurity support and services on behalf of the Commonwealth in the region, where only the Australian Government brand is used in service delivery.

105. As the Commonwealth efforts to support our region scales in Horizon 2 in terms of tempo and complexity, Government invests in additional measures to increase the numbers, seniority and technical abilities of Australian Government officials conducting and managing complex cyber programs and industry consortiums.

End Notes

[i] Nozomi Networks, July 2025, OT/IOT Cybersecurity Trends and Insights, 2025 1H Review; https://www.nozominetworks.com/resources/ot-iot-security-report-july-2025
[ii] Department of Industry, Science and Resources, April 2023, National Robotics Strategy Discussion Paper; https://consult.industry.gov.au/national-robotics-strategy
[iii] Office of the Australian Information Commissioner, Getting AI right benefits businesses, productivity and the community; https://www.oaic.gov.au/news/blog/getting-ai-right-benefits-businesses,-productivity-and-the-community
[iv] Department of Industry, Science and Resources, 30 April 2024, Leading quantum company chooses Australia as site for its groundbreaking utility scale quantum computer; https://www.industry.gov.au/news/leading-quantum-company-chooses-australia-site-its-groundbreaking-utility-scale-quantum-computer

Thales Australia Contributors: This submission was made possible by [redacted].