Telstra's Submission to Horizon 2 of 2023-2030 Australia's Cyber Security Strategy – Policy Discussion Paper

29 August 2025

Executive Summary and Recommendations

Telstra welcomes the opportunity to make a submission in response to the Department of Home Affairs Horizon 2 of the 2023-2030 Australian Cyber Security Strategy Policy Discussion Paper (the **Paper**). We continue to support the Australian Government's intention to uplift cyber resilience and boost cyber security across the economy.

Since the release of the 2023-2030 Australian Cyber Security Strategy (**Cyber Strategy**), there has been sustained momentum through legislative and policy settings and new initiatives towards whole-of-economy progress in making Australia more cyber resilient. Telstra has a long history of working in partnership with the Government on operational security and cyber policy issues, including in implementing various initiatives under the Cyber Strategy. In responding to the paper, we have selected those questions where Telstra is best placed to provide insight and expertise.

Our key recommendations:

- Using recent incident findings, focus on identified root causes of risky cyber behaviours to prioritise interventions and resilience initiatives.
- Prioritising solutions and initiatives that support intuitive security behaviours and encourage vendors to provide technology that is safe by default.
- Framing the cyber threat narrative around practical actions to improve resiliency for businesses and their supply chains.
- Government leaning into its important role as a strategic enabler of workforce capability, with a focus on embedding cyber literacy, enabling skills mobility, and supporting national workforce planning and critical role mapping.

Outlook for Horizon 2

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

Given the accelerating rapidity of change in the technology landscape, it is difficult to signpost with accuracy the trends or developments that will dominate in the next few years. We suggest that both Government and industry should continue to explore and invest in testing quantum use cases, while actively preparing to secure critical assets for a post-quantum world. Strategically, the Government should be focused on establishing appropriate guardrails for emerging technologies, while balancing the need for innovation and opportunity. Considering lessons learned from AI and the associated guardrails, can create a good baseline to strategically prepare for new technologies and trends on the horizon, across opportunities, risks, ethics and inclusion. We also suggest Horizon 2 should focus on addressing AI-specific threats and how effective mitigation strategies such as AI gateways or distributed exploit protection could be enabled to protect the digital ecosystem.

Shield 1: Strong Businesses and Citizens

What could government to do better target and consolidate its cyber awareness message?

What programs or pilots have been successful in this context? What additional supports could be developed or scaled-up to address these issues in partnership with both education stakeholders and those with technical cyber security expertise?

Using recent incident findings, we recommend focusing efforts on known root causes of risky cyber behaviours, to challenge assumptions that individuals and entities partake in such behaviours due to a lack of awareness or education. The proposed Cyber Incident Review Board will be instrumental in this work across the economy, and we are keen to see this established soon.

There has been increased focus and investment in campaigns promoting awareness of cyber security risks, however individuals continue not to engage in relatively simple protection mechanisms, such as applying multifactor authentication or changing compromised passwords. We recommend prioritising efforts on understanding why these behaviours persist and looking for solutions that allow for intuitive security experiences and encourage vendors to provide technology that is safe by default. Given the sustained efforts that have been made across government and industry in increasing cyber awareness, we would suggest evaluating whether increased levels of knowledge have equated to meaningful levels of change, and if not – why not?

We note that cyber literacy is an effective tool for individuals. The Paper states that research indicates females disengage from STEM subjects as early as primary school. There is an opportunity to scale tailored programs, such as those run by the Australian Women in Security Network and showcase diverse career opportunities. Further, where we know there are high levels of disengagement, we suggest that on an annual basis, a tailored program continues to be prioritised within the school curriculum about being cyber aware, scanning the horizon for emerging technologies and explaining associated risks.

How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)? How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience?

For many businesses, the first interaction with existing cyber resources is when the business has experienced an incident. To improve awareness and utility, we suggest promoting and providing the resources in a technology marketplace that serves as a one-stop-shop for SMBs to improve their security posture.

Further, there are multiple forums through industry and Government that highlight the importance of SMB security uplift. To increase uptake, we suggest connecting these SMB forums to other initiatives, such as those focusing on workforce or skills development.

What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFP's?

There is a notable gap for SMBs and NFPs who want a measurable benchmark to identify what best practice looks like and whether they have achieved it. For larger or more mature enterprises, there are multiple standards to choose from, such as NIST or ISO27001.

We suggest scoping down an existing cyber security standard (such as Essential Eight or SMB1001) to four key controls that are more manageable and memorable for SMBs to adhere to. Building on the work undertaken by the Executive Cyber Council's Small to Medum Business Working Group and the awareness campaign they ran (Stop the Hack), will also provide a minimum baseline of suggested actions to protect vulnerable small businesses.

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

We recommend a shift in messaging for individuals and smaller entities towards the practical actions to build resilience for themselves and their supply chain and partners. Framing the threat in terms of resiliency ensures that individuals and small businesses are better equipped to withstand and respond to the threat when it does occur.

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

We suggest that at a minimum the significant role that end-of-life devices and legacy systems can play in creating vulnerability to ransomware attacks should be made clear to Individual and small business consumers. These consumers may believe when they buy a device that security is ensured for the lifetime of the device when in fact the device requires regular security updates or patches.

To facilitate a stronger cyber security posture, the Government could also consider signposting end-of-life devices within a central repository (for example where patching support is no longer provided).

Which regulations do you consider most important in reducing overall cyber risk in Australia? Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?

The *Security of Critical Infrastructure Act 2018 (SOCI Act)* is one of the most important regulations in reducing overall cyber and broader security risks in Australia.

The telecommunications sector has enhanced requirements in Part 2D of the SOCI Act, including an obligation to protect critical telecommunication assets, notify the Department of Home Affairs about adverse changes to those assets and to maintain a Telecommunications Security Risk Management Program. The Government may choose to consider whether entities from other critical infrastructure sectors that are designated as Systems of National Significance should also have an elevated cyber maturity compliance requirement, given their criticality to underpinning systems and services for Australians.

Shield 2: Safe Technology

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

We welcome the publications and guidance made by the Australian Cyber Security Centre related to the security standards for smart devices. If information has been provided by vendors that updates are no longer being made and the software has been retired, consumers should be supported in understanding the risks from these products, to make informed purchasing decisions, such as in

online marketplaces. Consumers need to understand what a safe cyber security product is to ensure they can protect themselves.

What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?

The Foreign Ownership, Control or Influence Risk Assessment guidance and additional Directions indicating the risks associated with technology vendors have been helpful in validating and refining our supply chain governance processes and ensuring alignment with Australia's latest national security priorities. To the extent that Government can continue to be proactive and forward-leaning in providing clarity and specific guidance on risks in the technology supply chain, this supports improved security by enabling specialists such as engineers, software developers and procurement teams to confidently work within guardrails.

What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies? What do you consider to be the most serious national security risks presented by critical and emerging technologies, such as AI?

It is incredibly valuable for the Government to provide guidance on supporting the safe and responsible uptake of emerging technologies. As part of the work Telstra has been co-leading with the Tech Council of Australia in the Executive Cyber Council's Emerging Technology Working Group, we will be producing a report which considers the intersection of AI and Cyber, drawing on the experiences of senior leaders within the economy, to encourage entities to lead with an awareness of the risks and opportunities of new technologies. The intention is to create a product which provides a series of questions as an agnostic framework or lens through which to view new and emerging technologies. We would suggest evaluating the response from industry for this ECC product, to help inform any new guidance that the government provides on emerging technologies.

Additionally, as quantum technologies continue to develop, it would be useful if the Government were able to provide some guidance on how to assess these technologies, especially for smaller entities.

Shield 3: Threat Sharing and Blocking

What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry? Does the government need to scope and define what Australia's proactive cyber security posture should look like for industry?

Government could scope and define more specifically what actions can contribute to a more resilient cyber posture for businesses. Providing consistent and measurable benchmarks of what good looks like for industry can provide additional context for these targeted actions.

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

Requiring industry to block threats at scale, without regard to resources, experience or size is not a practical option. To strengthen the value of the Cyber Threat Information Sharing (CTIS) platform to industry, attention should focus on improving the quality of indicators that are shared.

Confidence in the quality of CTIS feeds can be improved by curating the indicators that are provided (or by providing both 'high-confidence' validated and 'lower confidence' unvalidated feeds) to help reduce validation workloads on consuming organisations and increase the usability of the platform for small-medium organisations. The human-validated stream should include the most important, timely and actionable threat intel indicators for action.

How could the use of safe browsing and deceptive warning pages be amplified?

We suggest that where deceptive warning pages are usually identified and reported to the relevant OTT provider only, this report should instead be redirected to a central coordination hub such as the National Anti-Scam Centre (NASC). This allows for the sites to be assessed by the NASC as deceptive, and then distributed among all OTT providers, to support protection at scale.

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

Sectors will often struggle to consume and act on threat information, without additional funding or resources. We suggest ISACs could focus on automating provision of threat information to security vendors and device manufacturers, operating in low-maturity sectors, so that threats can be blocked automatically at device & network level.

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

At a state emergency management level, roles and responsibilities are well-practiced and clear, such that for example, if a cyber-attack created power and communications outages or other consequences to critical services, there are robust pathways and processes for escalation and support.

However, in a conflict or crisis escalation with multiple and unpredictable cascading consequences, where a national-level response is required and/or entities are required to report incidents and disruptions to a national authority, there is inconsistent understanding across industry, and between industry and government, of where some roles and responsibilities sit. This extends both to understanding which agency or department would issue any direction or request to mitigate cyber risk or consequences, and how this instruction would be provided in a degraded communications' environment.

We are greatly encouraged by the focus from government on developing and testing crisis scenarios with critical infrastructure and partners across the wider economy. While cross-sector exercises are resource-intensive for participants, this is offset by the high value of the insights that can be generated.

We encourage government, as far as possible, to provide multi-agency collaborative government representation and leadership of national cross sector exercises at the strategic and operational level, to ensure all relevant parties of government are in the room and their roles and responsibilities are clear to industry. This will support clarity on escalation and communications pathways e.g. NOCS, Coordinator, ACSC, State Government bodies and prepare organisations for dynamic and trusted response in times of crisis.

How could government better incentivise businesses to adopt vulnerability disclosure policies? Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?

We suggest that vulnerability disclosure programs should be rebranded as a tool to safely report vulnerabilities and improve overall security. A national vulnerability disclosure program is worth exploring but would require sufficient resourcing and a clear responsive feedback loop.

Shield 4: Protected Critical Infrastructure

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

The SOCI Act applies a principled risk-based approach, recognising that critical infrastructure entities are best placed to protect their assets. The Risk Management Program obligations are relatively new, and yet to be enforced for the telecommunications sector. Further uplift and compliance will be supported by the ongoing development of example-based guidance materials and cross-sector and sector-specific forums.

As part of the enforcement activity that will happen in the following years, we suggest guidance is provided on thresholds for acceptable risk mitigations, e.g. adequate, good, exceeding, such that industry has signposts to build into their Risk Management Program and associated processes.

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

We appreciate the Government's consideration and extensive consultation in not duplicating regulatory burden on the telecommunications industry, by moving across the TSSR obligations into the SOCI Act.

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

We recommend a continuing series of scenario-based exercises, including scenarios that test understanding and application of the Foreign Ownership, Control or Influence (**FOCI**) guidelines.

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

We utilise the Protective Security Policy Framework (**PSPF**), relevant PSPF directions and PENs to support and inform our security processes.

Shield 5: Sovereign Capabilities

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

The Government has the opportunity to act as a strategic enabler of workforce capability, with a focus on embedding cyber literacy, enabling skills mobility, and supporting national workforce planning. We recommend embedding cyber literacy across the talent pipeline: Cyber should be treated as a foundational skill, integrated into school curricula, vocational education, and university programs—not just reserved for STEM pathways.

We recommend that the Government lead national workforce planning by coordinating a whole-of-economy approach to cyber capability, mapping current and emerging roles, forecasting demand, and aligning education and training systems accordingly.

To support mid-career transitions, we suggest the government should fund modular, stackable learning pathways and by recognising prior experience, government can help workers from adjacent industries transition into cyber roles.

By enabling skills-first hiring and credentialing, Australia's cyber workforce can be unlocked from hidden talent pools, where policies promote the recognition of micro-credentials and skills-based recruitment. We also suggest that by creating national talent pools, there could be shared platforms across and within sectors to draw from: for sourcing, training and deploying cyber talent.

To support industry growth, we suggest that the Government prioritises the following initiatives to enable agile workforce planning, skills development and cross-sector collaboration:

- Cyber portals and skills intelligence platforms: Centralised tools to map workforce gaps, retraining pathways, and labour market insights including evaluation of where options recognition of prior learning could be updated to better reflect the latest pathways into cyber security.
- Flexible learning models: Investment in modular, role-aligned learning pathways that support both entry-level and advanced transitions.
- Public-private forums: Co-design policy and regulation with unions, tech firms, academia, and government to ensure relevance and agility.

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

Telstra has seen success with several internal and sector-wide initiatives:

- Career Connect: Enables internal mobility by matching people to roles based on skills, not just job titles.

- Data & AI Academy: Offers targeted learning pathways for cyber, data, and AI skills—accessible to employees at all career stages.
- Hybrid work models: Flexible work arrangements have opened doors for diverse talent, including caregivers, regional workers, and those returning to work.
- Telstra has had some success with female-focussed programs to support diversity in talent pools through initiatives such as its targeted internship program, which it piloted with the support of the Australian Women in Security Network.

What are some of the industries with highly transferrable skill sets that could be leveraged to surge into the cyber workforce? Is there any existing research/data that could support these efforts?

Research from Telstra's workforce planning and external bodies like the Future Skills Organisation supports the transitions listed below, especially when paired with targeted learning interventions.

Industries with strong transferrable skills include:

- Telecommunications: Network engineers and infrastructure specialists already possess foundational cyber knowledge.
- Finance and insurance: Risk management, compliance, and data governance roles align well with cyber capabilities.
- Legal industry: Our Cyber teams have previously tapped into these domains with success - there are transferable skills
- Defence and emergency services: Operational discipline and security awareness are highly relevant.
- Retail and customer service: Increasing digitisation means frontline roles are becoming more tech-enabled, with potential for upskilling into cyber support functions.

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

We recommend establishing joint workforce strategy forums, that bring together HR leaders, educators and policy makers to align on future capability needs. We can drive innovation by funding collaborative pilots, for example by testing AI-enabled workforce planning tools or cyber skills bootcamps with shared evaluation metrics. By sharing evaluation metrics and workforce data through secure, anonymised data sharing, all parties would understand trends and respond proactively across the economy.

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

Strong research and data are necessary for good policy development, particularly where there is concern about the impact that technology will have on the workforce in general.

By embedding industry placements into academic programs, this can assist students to gain real world experience that improves employment outcomes. This can also be extended to supporting

cross-sector fellowships, which enables academics to work within industry and vice versa fostering mutual understanding and collaboration.

We also reiterate the benefit in co-developing micro-credentials, which are agile, role aligned and allow for stackable credentials that support lifelong learning and career transitions.

How would we best identify and prioritise sovereign capabilities for growth and development across government and industry?

A national capability mapping exercise would be useful in identifying the cyber skills and capabilities that are critical to national security and economic resilience. An assessment of which of these capabilities must then be retained in house and those that can be outsourced or automated will help define the sourcing guardrails to prioritising sovereign capabilities. We also suggest aligning funding to strategic skills, so that investment is prioritised in areas like secure software development, cloud security and incident response.

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

Our key concerns include an over reliance on external vendors, which can limit internal capability growth and pose sovereignty and innovation risks. In addition, Australia has an ageing workforce in critical roles, which means without considered success planning, knowledge loss is a real threat. On the opposing side of the spectrum, skills bottlenecks are prevalent in emerging technology where roles in Quantum and AI are evolving faster than training pathways.

In response our suggested mitigation strategies include:

- Investing in internal capability building: Shift from outsourcing to in-house development where it makes sense; leverage external partnerships where this can accelerate capability growth to the benefit of the whole business.
- Embedding skills-based succession planning: Identify critical roles and ensure knowledge transfer.

Shield 6: Strong region and global leadership

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

We consider that the use of attributions, advisories and sanctions is an effective tool in cyber diplomacy. We encourage strengthening international partnerships particularly in the Pacific and Southeast Asia, to reinforce deterrence activities.

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

Continued alignment of global software and network security standards will encourage secure by design products that promote simplicity and interoperability.

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

It is important to evaluate and identify truly leading global best practice regulatory frameworks or requirements with which to align Australia's efforts. The domestic context and strategic priorities of each country are different, for example, attempting to align with more prescriptive requirements in the UK or Singapore, may not achieve the same outcome in Australia or could require significant shift in resourcing focus and ways of working.