Australian Government

Charting New Horizons

Developing Horizon 2 of the 2023–2030 Australian Cyber Security Strategy

Policy Discussion Paper

Minister’s foreword

The world around us is changing fast, and nowhere is that more evident than in the online space we rely on for all aspects of our lives. Staying safe online is an evolving challenge for every Australian, with one cybercrime, on average, reported every six minutes. The rise of Artificial Intelligence will only increase that threat. That’s why, as Australia’s Minister for Cyber Security, I am committed to creating a digital environment that is safe, trusted and secure.

Globally, we’re facing some of the most serious challenges since the Second World War. Now, more than ever, we need robust and reliable cyber security foundations in place to disrupt and deter criminals and allow individuals and businesses to bounce back from cyber attacks. This will take a whole-of-economy and whole-of-nation approach, centred on a partnership between industry and government.

We shouldn’t forget cyber security also presents an opportunity for Australia to be a leader in the growing global industry, with the chance to create well-paid jobs and products that can be exported around the world.

By striving to be a world leader in cyber security, we will further strengthen the foundations for Australia to be recognised as a top destination for cyber security talent, leveraging our position to lead cyber research, innovation and entrepreneurship.

In November 2023, the Australian Government released the *2023-2030 Australian Cyber Security Strategy* to build national cyber resilience and boost cyber security across the economy. As we move into the next phase, we want to continue our collaboration with you on the next series of outcomes, actions and initiatives needed to move our cyber security forward. Through Horizon 2, we will seek to ensure that Australia’s regulatory, legislative and policy settings seize the opportunities of technological advancements, while protecting our national interests.

This discussion paper is an opportunity for you to provide your views on what outcomes we need to achieve collectively. By 2028 we want to further embed cyber messaging, standards capability and efforts across society, empowering our businesses and citizens to protect themselves.

We also want to have established Australia as a trusted and influential global cyber leader, working with international partners to build a cyber resilient region. That will bring together the best of Australian values; collaboration, innovation and an unwavering commitment to protecting what matters most.

The foundations we have laid under Horizon 1 will be enhanced and expanded over the next Horizon to secure Australia’s digital future for generations to come.

The Hon Tony Burke MP
Minister for Home Affairs
Minister for Cyber Security

Table of Contents

Introduction

In November 2023, the Australian Government released the *2023-2030 Australian Cyber Security Strategy* (the Strategy) and Horizon 1 Action Plan with a bold vision for Australia to be a world leader in cyber security by 2030.

The Strategy called for a new era of collaboration between industry and Government to keep Australia's digital frontier safe, secure and prosperous. Twenty months into this journey, we are seeing significant momentum across a range of cyber reforms, programs and initiatives.

The Strategy is structured around six 'cyber shields' to help defend our citizens and businesses from cyber threats and to take economic and productivity opportunities that cyber security offers Australia.

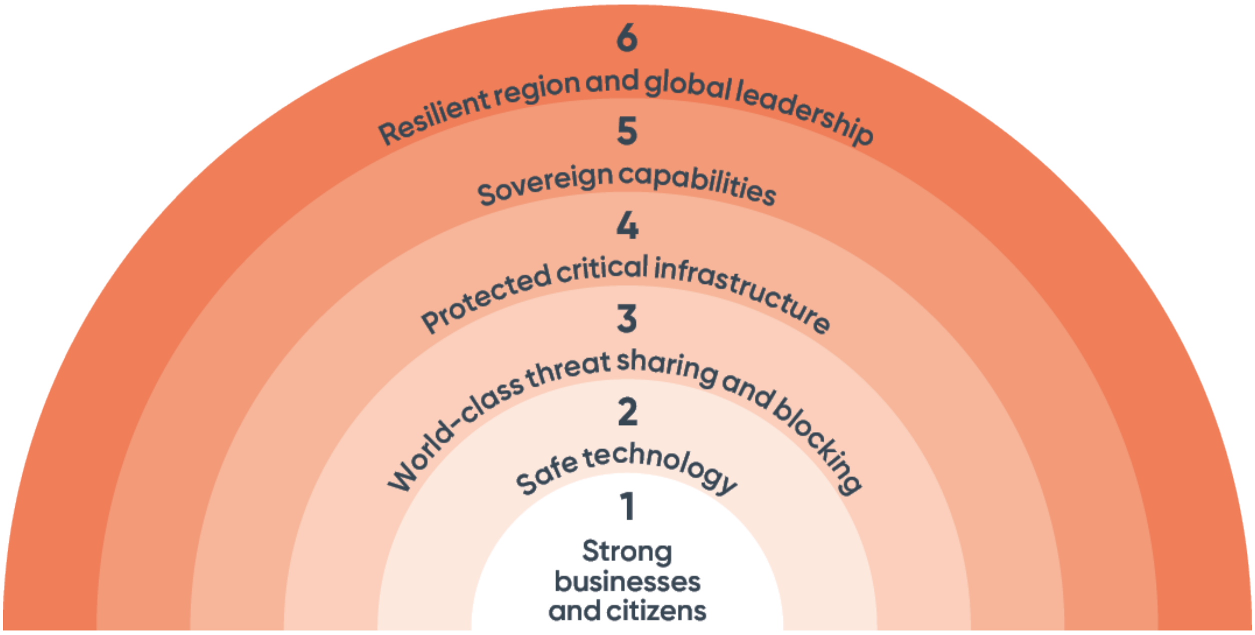

6
Resilient region and global leadership
5
Sovereign capabilities
4
Protected critical infrastructure
3
World-class threat sharing and blocking
2
Safe technology
1
Strong businesses and citizens

Figure 1. Cyber shields

Acknowledging the fast evolving nature of cyber security and the changing threat landscape, the Strategy established a phased approach to delivery through an Action Plan across three separate time horizons.

As we complete Horizon 1 and embark on Horizon 2, it is important to reflect on what has been achieved under the Strategy and define future possibilities. Horizon 1 set the foundations for national reform and addressed critical gaps. In Horizon 2, we will scale cyber maturity across the whole economy.

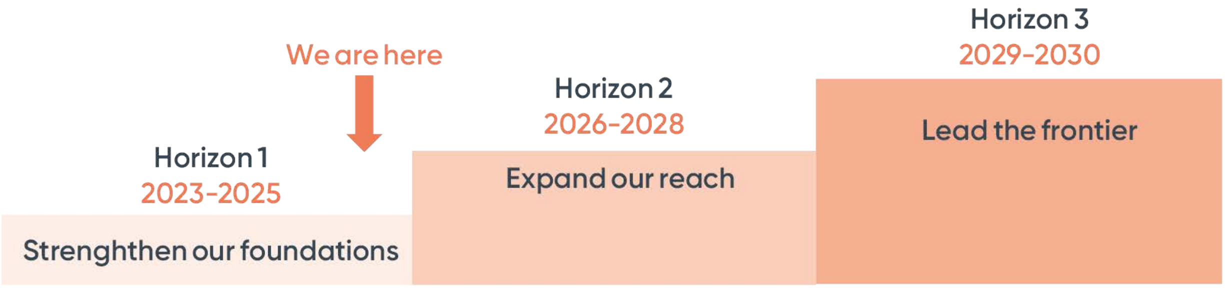


Figure 2. Action Plan horizons

The purpose of this Discussion Paper is to continue our collaboration with businesses and citizens on identifying and developing policy options that will best position Australia to be a cyber-resilient nation, and to explore how to work together to achieve them over the next Horizon.

The paper is divided into three parts:

- **Part 1** provides an update on the implementation of Horizon 1 of the Strategy.
- **Part 2** sets out the Government's framing and potential areas of focus for Horizon 2. It also presents our evaluation methodology for the Strategy.
- **Part 3** provides a shield-by-shield level view of Horizon 2 and poses a number of discussion questions.

Engage with us

We welcome responses to the questions outlined in this Discussion Paper (consolidated at **Appendix A**) and any additional matters relevant to the Strategy by **29 August 2025**.

Please send any questions to:
CSSH2@homeaffairs.gov.au

Submissions should be made in PDF via the Horizon 2 Discussion Paper webform at:
homeaffairs.gov.au

This Discussion Paper is only the first step in our consultation on Horizon 2. There will be further opportunities to engage with us, including on the development of specific actions and initiatives to achieve these outcomes.

Please see our website **homeaffairs.gov.au** to keep up to date and for a schedule of other engagement forums to continue the discussion, such as live online town halls.

1. Horizon 1: A national approach to cyber security

Horizon 1 of the Strategy, realised through the Horizon 1 Action Plan, comprised 60 individual initiatives led by agencies across the Australian Government. To date, all initiatives are on track for delivery by the end of 2025 (as at 30 June 2025).

A detailed summary on the progress of all of the Horizon 1 initiatives is provided in **Appendix B**.

1.1. Key achievements under Horizon 1

Implementing Australia’s landmark *Cyber Security Act 2024*

On **29 November 2024**, the Cyber Security Legislative Package - encompassing the *Cyber Security Act 2024* and amendments to *the Intelligence Services Act 2001* and *Security of Critical Infrastructure Act 2018* - became law. Measures introduced through the Package implemented a number of initiatives under the Strategy and include:

- powers to mandate minimum cyber security standards for smart devices (***Shield 2***);
- introduction of mandatory ransomware reporting for certain businesses to report ransom payments (***Shield 1***);
- introduction of a ‘limited use’ obligation for the National Cyber Security Coordinator and the Australian Signals Directorate (ASD) (***Shield 1***);
- establishment of a Cyber Incident Review Board (***Shield 1***);
- alignment of telecommunication providers to the same standards as other critical infrastructure entities (***Shield 4***);
- enhanced protection of the critical data held, used and processed by critical infrastructure (***Shield 4***);
- introducing a review and remedy power for Risk Management Programs (***Shield 4***); and
- expanding crisis response arrangements to ensure they capture secondary consequences from significant incidents (***Shield 4***).

Cyber security awareness campaign

The ‘*Act Now. Stay Secure.’* campaign aims to build a baseline cyber security capability for all Australians. Phase 4 of the campaign launched on **11 May 2025** and remains in market. The campaign is driving behavioural change by empowering Australians to take control of their cyber security by adopting simple cyber safe actions to protect themselves online.

Tackling ransomware

Under Horizon 1 there were a number of initiatives aimed at disrupting, deterring and supporting Australian businesses to bounce back from ransomware attacks.

On **10 October 2024**, the Minister for Home Affairs launched the Ransomware Playbook on the cyber.gov.au website. The Ransomware Playbook provides industry with clear information on how to prepare for, respond to and recover from a ransomware incident. The interactive tool includes easy-to-use guides such as a cyber security checklist for small businesses, advice on securing devices against a ransomware attack, and guidance for incident response planning.

From **30 May 2025**, the Ransomware Payment Reporting Regime commenced under the *Cyber Security Act 2024*, which will support Government to better understand the prevalence of ransomware attacks across the economy to help provide more targeted support to victims and develop policy solutions in the future.

The Government has also continued its focus on supporting and driving international disruption and deterrence programs through the Counter Ransomware Initiative (CRI).

Commonwealth Cyber Security Uplift

Horizon 1 outcomes include fundamental reform to the *Protective Security Policy Framework*, and the delivery of five directions to manage emergent risk to the Commonwealth and provide strong foundations to improve the Commonwealth's cyber security resilience and risk management posture.

In **July 2025**, the Department of Home Affairs released tranche 2 of the Commonwealth cyber security uplift reforms, which comprised key policies and standards to address key risk in risk management prioritisation and investment. This included introduction of the *Systems of Government Significance Standard*, *Australian Government Gateway Security Standard* and commencement of reforms to the *Hosting Certification Framework*.

Cyber security for Australia's aviation and maritime transport sectors

On **27 March 2025,** the *Transport Security Amendment (Security of Australia's Transport Sector) Act 2025* received Royal Assent and became law. The Act updated and strengthened security frameworks in response to evolving threats to the transport sector and incorporated recommendations from a review of Australia's aviation and maritime transport security settings.

The Act also introduced mandatory reporting of cyber security incidents related to the transport sector, reflecting the increasing importance of cyber security in protecting Australia's critical infrastructure.

Grants to support cyber security uplift and Australia's cyber workforce

Under Horizon 1, the Government initiated a number of grants programs to support industry in the development of policy ideas, to pilot initiatives and to support amplification of cyber security messages across the economy.

In **December 2024**, the Government announced that over 200 funding recipients ($9.6 million) through the **Cyber Security Awareness Support for Vulnerable Groups grants program** to uplift cyber awareness amongst vulnerable communities in Australians.

In **January 2025**, the Government awarded the **Health Sector Information Sharing and Analysis Centre** grant to the Critical Infrastructure Information Sharing and Analysis Centre (CI-ISAC) to facilitate ongoing industry-to-industry threat intelligence sharing within the health sector ($6.361m GST exclusive).

In **June 2025**, the Government awarded the **Labelling Scheme for Smart Devices** grant to IoT Alliance Australia to implement an industry-led and internationally aligned voluntary labelling scheme for consumer-grade smart devices in Australia ($1.7 million).

In **January 2025**, applications closed for the **Growing and Professionalising the Cyber Workforce Cyber Security Industry** grant. Applications are now progressing through the final assessment process. The grant will provide $1.9 million in funding to support industry engagement to design, promote and pilot a professionalisation scheme for Australia's cyber security workforce.

Cyber incident management and preparedness

The National Office of Cyber Security (NOCS) has delivered whole-of-government coordination and support to 98 cyber incidents. The NOCS has also delivered 20 exercises across a range of sectors, and with government, and has participated in a range of industry-led sector and internal exercises, and published nine sectoral cyber incident playbooks.

Executive Cyber Council

In **November 2023**, the inaugural meeting of the Executive Cyber Council (the Council) was convened. The Council meets biannually and plays an important role in facilitating genuine and transparent co-leadership with industry on key cyber security issues. The Council also supports the delivery of national cyber security priorities, including industry representatives leading working groups focussing on emerging technology, sovereign cyber capabilities, cyber workforce, and small and medium businesses.

National Cyber Intel Partnership

The National Cyber Security Coordinator chairs the National Cyber Intel Partnership (NCIP). The NCIP convenes Australian Government and industry stakeholders quarterly to discuss approaches to support cyber threat intelligence sharing and inform the deployment of threat blocking capabilities that can prevent identified threats from reaching end users.

The NCIP is operationalised through a Threat Blocking Working Group which is driving three innovative pilots led by key industry threat blockers in Australia.

Securing data and technology

The Government has worked with industry and academia to support development of data security frameworks and address risks to Australian technology associated with foreign ownership, control or influence.

In **December 2024**, the Minister for Home Affairs announced the finalisation of the *Technology Vendor Review Framework*. The Framework provides Government with a process to consider foreign ownership, control or influence risks associated with technology vendors.

The Department is also working with CSIRO Data61 and industry stakeholders to research and develop a voluntary data classification framework. This framework aims to help industry identify, assess and communicate the value of their data holdings.

International cooperation on cyber response

Since **January 2024**, Australia has imposed **four sets of cyber sanctions** (complemented by parallel sanctions issued by the US and UK and supported by a number of international partners) to respond to cybercriminal activity. This included Australia’s first cyber sanction (Aleksandr Ermakov; 23 January 2024).

Australia has also joined **nine technical advisories** attributing malicious cyber activity to state-affiliated actors, and issued Australia’s first ASD-led technical advisory (joined by the US, UK, Canada, New Zealand, Germany, Japan and ROK) attributing malicious cyber activity to a state-sponsored actor (APT40, China’s Ministry of State Security; 9 July 2024). Australia has issued **four statements of support for attributions** made by other countries, and one statement of support for the EU’s imposition of sanctions on three individuals linked to the Russian Armed Forces for their role in malicious cyber activity targeting Estonia.

The Australian Government has established a regional cyber incident response function - Cyber Rapid Assistance for Pacific Incidents and Disasters (RAPID). This function has supported Pacific island countries to strengthen their cyber resiliency. To date, we have **deployed RAPID ten times to assist major incidents and events**, and worked with countries ahead of cyber incidents to build their preparedness.

Our capacity-building program for the Pacific and Southeast Asia has also been refreshed, with the development of the SEA-PAC Cyber Program (2024-28).

2. Developing Horizon 2

Increasing tensions in our society, geopolitical competition and technological advances have created a multifaceted, cascading and compounding threat environment. Simultaneously, reliance on the digital economy is rapidly increasing – a growth that has been matched by emerging vulnerabilities in cyber security.

Emerging technologies such as quantum and Artificial Intelligence (AI) provide both opportunities and increased risk to our economy. As we move into Horizon 2, it is paramount that we harness the efficiencies and capabilities that are offered through these technologies while continuing to protect Australia's data and technology assets from malicious actors.

Working with industry, the Government wants to ensure that all parts of our society are equipped with simple and easy-to-follow cyber security guidance and standards to navigate the digital domain.

Looking towards Horizon 2, the Government is exploring policy ideas and programs that allows Australia to:

- **Embed** cyber security messaging, standards, capability and efforts across society, from our homes and schools to our businesses and government partners;
- **Empower** business (particularly small business), not-for-profits and citizens to protect ourselves and each other, reducing the barrier for applying protective frameworks ensuring Australian businesses are more productive and bounce back quicker; and
- **Enhance** our cyber regulatory frameworks through structural reforms to harmonise and simplify regulation, strengthen our cyber workforce and business ecosystem and better coordinate security outcomes for Government cyber uplift.

2.1. Outlook for Horizon 2

By 2028, Australia will be facing a materially different cyber security landscape. Both in terms of the threats facing our community and economy, as well as the opportunities that will open up with new technology and digital transformation. While it is difficult to pinpoint with any accuracy how these changes will materialise, it is clear that the cyber security needs of Australian businesses and citizens will have increased exponentially. As an example, in 2023 there was an average of 24 connected devices per Australian household. This is expected to grow to 32 connected devices per Australian household by 2027, or an equivalent increase of 109 million devices in Australia from 2023 to 2027.[1]

Australia's increasing adoption of digital technology coupled with increased online investment and digitisation will unlock significant social and economic opportunities, but equally will contribute to creating a larger attack surface for threat actors. This will have a corresponding cost to the economy and impact on the security of individuals and businesses. Government's internal research indicates that while cyber incidents will cost the Australian economy an estimated $25.4 billion in 2025-26, they are projected to cost an estimated $215 billion over the next 10 years.

Threat actors and criminals are continuing to evolve their business models and are becoming bolder in their attacks on Australian businesses and citizens. As we move into an era of increased geostrategic competition, the volume, speed and sophistication of cyber attacks will be expected to increase. ASD data shows that in Australia there was one cybercrime report every six minutes in 2023-24.[2] The average cost for cybercrime borne by small businesses has increased by eight per cent, indicating criminals targeting our most vulnerable businesses.[3]

[1] Telsyte, Telsyte Australian Smart Home Market Study 2023, accessed 5 June 2025, https://www.telsyte.com.au/announcements/2024/3/20/australias-smart-home-market-set-to-crack-25b-driven-by-ai-energy-savings-and-security

[3] Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC), Annual Cyber Threat Report 2023-24, accessed 7 June 2025, https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

[3] Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC), Annual Cyber Threat Report 2023-24, accessed 7 June 2025, https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

Taking this lens, across Horizon 2 we want to achieve an end-state in 2028 where:

- Our **citizens,** particularly vulnerable Australians, are educated about cyber security risks and motivated to take action to reduce risks to themselves and their communities. Australians can make informed decisions about the digital tools they bring into their homes, and are confident about the authenticity and reliability of their online activities and the technologies they choose to use.
- **Small and medium-sized businesses and the not-for-profit sector** are increasingly educated and motivated about cyber risks, digital tools and online activities and have access to suitably designed standards that are cost effective to implement and provide a simple and clear pathway to uplift their cyber resilience.
- **Large business** is deploying their best efforts on cyber security in Australia and have access to an abundant and diverse cyber security workforce with the skillsets to start solving tomorrow's problems today. Security-by-design and security-by-default is incorporated appropriately into business practices, supported by harmonised and simplified cyber regulation.
- The cyber security of our **critical infrastructure** has been uplifted to a meaningful standard, supported by a mature regulatory position from Government ensuring non-compliance is identified and rectified.
- **Federal, state and local governments** are working together to maintain the resilience of online government services and systems. The Australian Government is an exemplar in cyber security leadership and data protection.
- **Australia remains a cyber partner of choice in the region**. We continue to shape, uphold and defend international cyber rules, norms and standards, and effectively impose costs on state and non-state malicious actors.

Question(s) to consider:

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

2.2. Collaborating across all levels of Australian Government

We understand the Australian Government also needs to continue to work closely with our State and Territory Government partners as joint stewards of Australia's government response to cyber security.

Our capacity as a nation to implement economy-wide resilience and uplift will depend on collaboration to ensure our work is delivered across Australia.

Horizon 2 provides an opportunity to set shared objectives for nationwide cyber security and resilience across all governments, including collaboration to uplift the cyber security of local government agencies. This environment of reliability and trust requires governments across Australia to continue to work together with industry and citizens.

Question(s) to consider:

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

2.3. Monitoring progress in a changing world—a framework for delivering cyber security outcomes

In Horizon 2, we will enhance our capacity to use data and evidence to deliver impactful policy in a dynamic and complex cyber security environment. We cannot wait until the end of the Strategy to assess its effectiveness. We must build timely feedback loops to ensure responsiveness to change.

The Australian Government is creating a world-first framework for conceptualising, measuring and analysing the impact of the Strategy. The first step is to define our long-term objectives. During Horizon 1, we have mapped the outcomes expressed in the Strategy and the interventions we expect will produce which outcomes, as part of a 'Cyber Security Policy Evaluation Model' (Figure 4). The Model will guide both the selection of interventions and the monitoring and evaluation of their effectiveness. Our goal is to develop a model that is long lasting and drives shared action beyond the current Strategy.

The basic building blocks (Figure 3) of the Model are:

1. **High-level expected outcomes** represented by solid circles. This includes both the outcomes we are trying to achieve (orange) and those we are trying to avoid (dark grey).
2. The **interventions** we expect will achieve those outcomes represented in open circles.
3. The **links** between interventions and outcomes, or our causal hypotheses, represented by arrows.
4. The **North Stars** represented by blue stars, are outcomes that are our ultimate goals and what success looks like. These points also represent the key outcomes for which we need to build data points and metrics for impact monitoring and ongoing whole-of-economy evaluation activities.

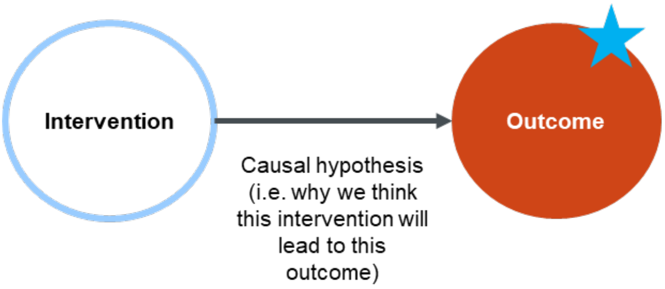

Intervention
Outcome
Causal hypothesis (i.e. why we think this intervention will lead to this outcome)

Figure 3. Building blocks of the Cyber Security Policy Evaluation Model

Once we have a Model agreed amongst our partners, the next step is to leverage the data architecture required to provide ongoing feedback and build a longitudinal picture of our progress. Identifying metrics to monitor these outcomes will not be easy; we cannot, for example, survey cyber threat actors about their motivations and plans. We are keen to develop metrics, and address data and evidence gaps in partnership with industry, academia, data agencies, and the community.

Question(s) to consider:

3. *Does the high-level Model resonate and do you have any suggestions for its refinement?*
4. *Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?*

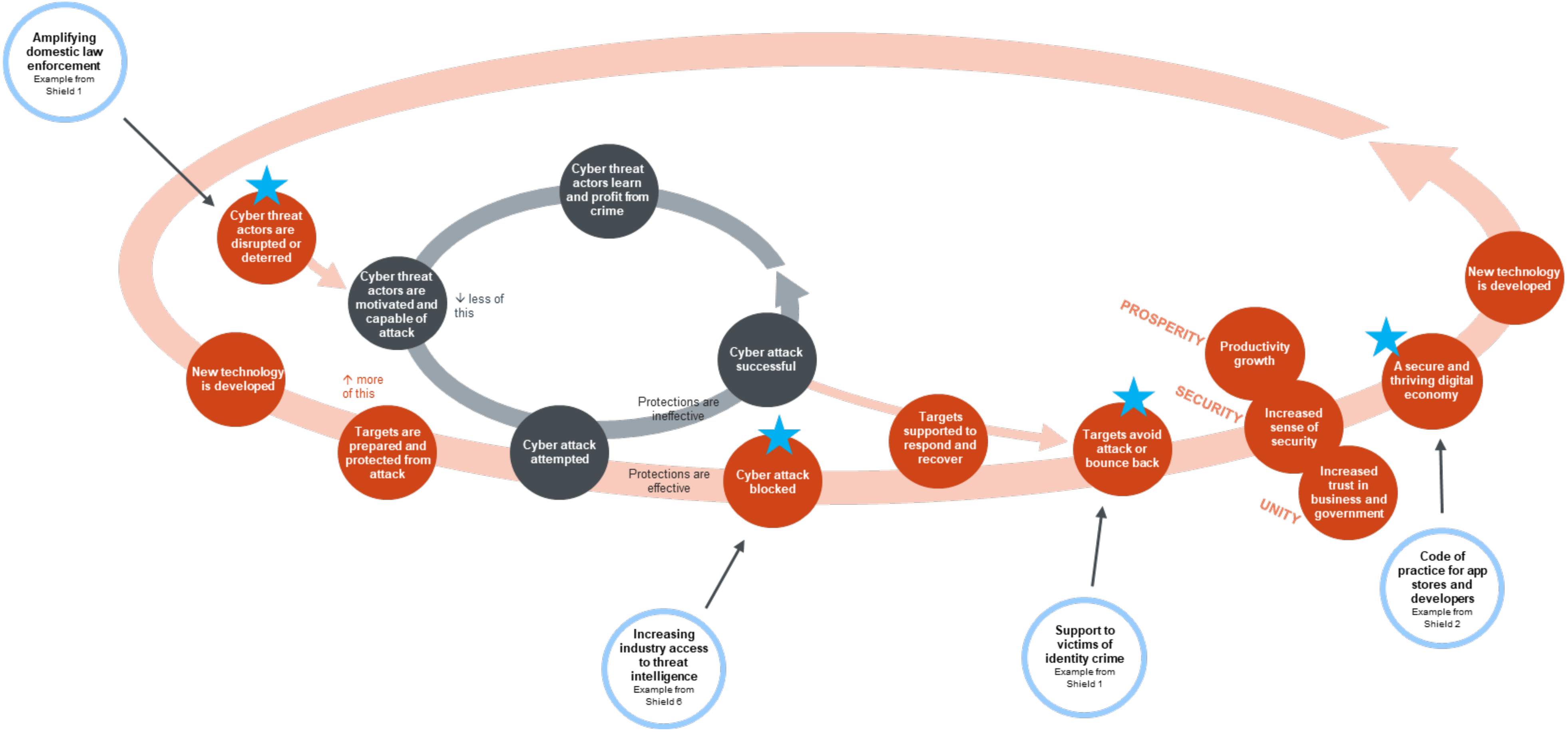

Amplifying domestic law enforcement
Example from Shield 1
Cyber threat actors are disrupted or deterred
Cyber threat actors learn and profit from crime
Cyber threat actors are motivated and capable of attack
↓ less of this
Cyber attack successful
New technology is developed
↑ more of this
Targets are prepared and protected from attack
Cyber attack attempted
Protections are ineffective
Protections are effective
Cyber attack blocked
Targets supported to respond and recover
Targets avoid attack or bounce back
PROSPERITY
SECURITY
UNITY
Productivity growth
Increased sense of security
Increased trust in business and government
A secure and thriving digital economy
New technology is developed
Increasing industry access to threat intelligence
Example from Shield 6
Support to victims of identity crime
Example from Shield 1
Code of practice for app stores and developers
Example from Shield 2

Figure 5. Cyber Security Policy Evaluation Model

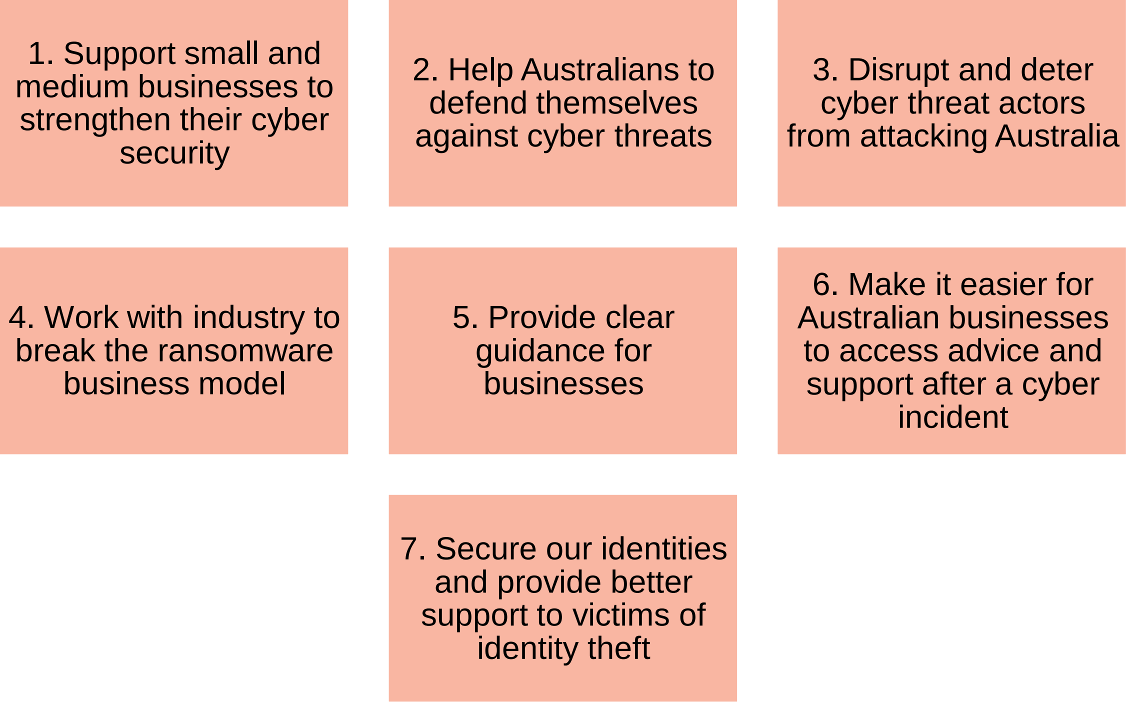
3. Shield-level focus for Horizon 2

The Strategy established six ‘cyber shields’ to drive uplift of Australia’s cyber maturity. Horizon 2 will take forward new initiatives under the six shields established by the Strategy.

We have outlined key areas of focus for each cyber shield to support stakeholders to respond to this Discussion Paper and provide ideas and suggestions.

3.1. Shield 1: Strong businesses and citizens

For Horizon 1 of the Strategy we focused on Shield 1, with 17 initiatives across seven different ‘action areas’.



1. Support small and medium businesses to strengthen their cyber security

2. Help Australians to defend themselves against cyber threats

3. Disrupt and deter cyber threat actors from attacking Australia

4. Work with industry to break the ransomware business model

5. Provide clear guidance for businesses

6. Make it easier for Australian businesses to access advice and support after a cyber incident

7. Secure our identities and provide better support to victims of identity theft

Figure 6. Shield 1 action areas for Horizon 1

For Horizon 2, we propose to build upon the successes of the seven Action areas developed for Horizon 1 under Shield 1, with a particular focus on five key outcomes.

Key areas of focus for Shield 1				
Consolidate our cyber awareness messages across the economy	**Increase cyber literacy in school programs**	**Target resilience uplift to small entities that cannot adequately protect themselves, including through giving small business clear and low or no-cost cyber standards to apply**	**Enhance support for citizens and victims of cybercrime to help them bounce back quicker**	**Harmonise and simplify cyber regulation to promote best practice and efficiency**

Unfolding Shield 1 focus areas for Horizon 2

Consolidate our cyber awareness messages across the economy

As technology rapidly advances and we spend more time online, individual Australians remain vulnerable to cyber attacks. First Nations people, older Australians, Australians with a disability, and those from a Culturally and Linguistically Diverse background are particularly vulnerable groups within the community. Many online users still report not using simple yet effective online safety strategies to protect themselves online. Emerging evidence shows the effectiveness of practical action-oriented messages in promoting online safety behaviours and reducing the harm from cybercrime.

Australians must be empowered to take control of their cyber security by implementing key cyber safe behaviours. The '*Act Now. Stay Secure.'* campaign is educating Australians on the simple cyber safe actions that everyone can take every day to protect themselves online. The campaign is targeted at all Australians, and includes tailored content for vulnerable groups. This campaign complements existing guidance and advice available on cyber.gov.au.

Question(s) to consider:

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

Increasing cyber literacy in our schools

Strengthening cyber security through education is one way we can target two key areas of focus; to support the upcoming generations and our greatest users of technology to keep themselves cyber safe, and to set foundations for a future pipeline of skilled and talented cyber security professionals.

Research has found that female students start disengaging from some STEM subjects as early as primary school. They only make up about a quarter of enrolments in Year 12 information technology, physics and engineering classes. Targeted programs in school settings could enhance greater diversity and talent pipelines for Australia's cyber workforce (a key focus of Shield 5). There are a number of such programs that have been piloted across Australia and in different contexts that provide a useful evidence base to consider for scalability and sustainability.

Question(s) to consider:

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

Target resilience uplift to small and medium-sized entities that cannot adequately protect themselves, including through low or no-cost standards to apply

Small and medium-sized businesses (SMBs) are increasingly vulnerable to cyber security incidents. Many SMBs and other small entities, including not-for-profit organisations (NFPs) are under-protected. These small entities often lack the capability and resources to navigate the current cyber landscape and deal with cyber incidents. This cyber maturity gap continues to widen.

As SMBs form part of the critical infrastructure supply chain, this represents a vulnerability in our national cyber resilience. When SMBs fall victim to cybercrime, it disrupts business activities and continuity, increases business expenses, and impacts their reputation and revenue.

Feedback from industry and SMB associations highlighted that further support is needed to address critical cyber vulnerabilities and prepare for emerging threats and challenges. We have heard a strong call to action to make it easier for SMBs and NFPs to access the advice and services they need. We need to drive uptake of security measures that will enhance whole-of-economy cyber maturity and resilience.

Question(s) to consider:

7. *How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?*
8. *How can industry at all levels and government work together to drive the uptake of cyber security actions by SMBs and the NFP sector to enhance our national cyber resilience? What type of support would be useful and who should provide it?*

Exploring cyber security standards for small businesses and not for profit

We have heard that a number of existing cyber security standards are not focused on the needs of smaller entities. They are generally designed to address cyber security in larger organisations and are challenging for smaller entities to implement. Industry feedback indicates the difficulty or inability to meet these standards as a major barrier in addressing cyber security vulnerability. Feedback suggests a government and industry-endorsed cyber security standard tailored for SMBs and NFPs would greatly assist in achieving national cyber maturity uplift.

Any new cyber security standard and supporting framework should be tailored to the diverse needs of smaller entities, including those in the NFP sector. It could then be accompanied by fit-for-purpose guidance and targeted assistance. The goal is to provide pathways for smaller entities to build their cyber maturity. By enhancing cyber security in SMBs and the NFP sector, Australia could increase participation in the digital economy and drive productivity growth, while also securing supply chains and the broader cyber ecosystem.

A new fit-for-purpose cyber security standard could also provide a certification pathway. A formal certification process could simplify cyber security uplift for SMBs, enable risk based approaches to cyber security and make it easier for all organisations to better secure their supply chains.

Question(s) to consider:

9. *What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFPs? What role should government play in supporting/endorsing SMB tailored standards?*

Additional cyber security challenges for the NFP sector

NFPs hold large volumes of sensitive data yet often lack adequate cyber security, making them attractive targets for malicious actors.

Some NFPs, particularly smaller entities, face a range of unique challenges in implementing robust cyber security protections. NFP workforces are highly reliant on volunteers. This can limit their ability to embed a strong security culture through ongoing training and awareness raising initiatives. The sector concurrently faces pressures to reduce spending on non-mission focused operations including administration and cyber security.

Public trust is a necessity for NFPs to continue delivering critical services while also encouraging financial, resource and time, contributions from the community. Ongoing cyber security uplift and resilience is essential to ensure NFPs maintain public confidence in the security of both their sensitive data holdings, as well as donor information.

Question(s) to consider:

10. *What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?*

The role of cyber insurance in strengthening cyber resilience for businesses and NFPs

Cyber insurance contributes to the broader resilience of business and NFP sectors, facilitating faster response and recovery from cyber attacks. In Australia, cyber insurance providers generally offer access to a suite of services and third-party providers, providing subject matter expertise and resources that would ordinarily be out of reach for smaller entities.

We have heard many Australian businesses have difficulty accessing cyber insurance, or see it as too expensive. The complexities or technical requirements of insurers could also be a deterrent, particularly to SMBs, where they may be unable to meet the cyber security standards applied to larger enterprises.

The market for cyber insurance in Australia is dynamic and evolving. Any interventions from Government need to be carefully considered to not distort the market or inadvertently affect pricing. However, there is a potential role for Government to better support availability of cyber insurance products, particularly for SMBs.

Question(s) to consider:

11. *Do you consider cyber insurance products to be affordable and accessible, particularly for SMBs? If not, what factors are holding back uptake of cyber insurance?*

Ransomware and cyber extortion

Ransomware continues to pose a significant threat to Australia's economy and critical infrastructure. Attacks are increasing globally, with Australia consistently ranking amongst the ten most targeted countries. Around one in 20 online Australians reported being a victim of ransomware or ransomware-related data theft and extortion. Of particular concern, SMBs are more likely than larger businesses to be targeted multiple times.

The Australian Government has implemented a number of measures in response, including a suite of free online resources designed to support individuals and business. These include the recently developed Ransomware Playbook, and Ransomware Prevention and Emergency Response Guides hosted on cyber.gov.au. Government has also invested additional funding under the Strategy into Operation Aquila, a joint initiative between the Australian Federal Police and the Australian Signals Directorate, to prevent, detect, deter and disrupt cybercriminal syndicates that target or threaten Australian Government entities, critical infrastructure and systems of national significance.

These efforts are further supported through the new data that Government will receive from the mandatory ransomware payment reporting regime, and the international advocacy that Australia provides as a leading contributor to the Counter Ransomware Initiative (CRI). The CRI brings together over 70 member countries to coordinate combatting ransomware threats.

Question(s) to consider:

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

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

Enhance support for citizens and victims of cybercrime to help them bounce back quicker

Not all individuals in Australia face the same challenges in building and maintaining their cyber resilience, some cohorts are more vulnerable to cyber threats. These cohorts may include LGBTQIA+ communities, First Nations, low socio-economic status, elderly or people with disabilities.

Of course, these cohorts are not viewed as one and they contain enormous breadth of diversity and individuality within them. Supporting all Australians to be empowered and contribute to our collective cyber resilience will benefit from an intersectional approach and the acknowledgment that each Australian's experience is shaped by unique challenges.

Across all levels of Government, there are a range of initiatives seeking to protect vulnerable cohorts' digital experiences. Through Horizon 2, we are interested in hearing ideas on policy options that would enhance or scale successful programs or target support for particularly vulnerable cohorts.

For example, an area of focus is on gender-related cyber security threats. The Government has committed to a range of initiatives in response to technology-facilitated gender based violence (TF-GBV). We are eager to understand cyber security mitigations that could hinder, halt or expose TF-GBV. This could include a range of policy or program ideas as well as technological solutions to develop ways to detect 'stalkerware' that may be installed on a device without the user of the device providing consent.

Question(s) to consider:

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

Strengthening Australia's identity crime response by scaling victim support and exploring systemic protections

Cyber incidents that expose personal information used for cybercrimes, including identity crime, are becoming more common. Identity crime is often an enabler of other crime types and, without swift remediation action, can cause severe and long-term secondary harms to victims, including significant financial loss and identity takeover. Even with the best efforts to deter and prevent identity crime, the tactics and techniques used by malicious actors evolve. This means it is impossible to educate and guard against every identity crime. This heightens the risk that all Australians could potentially be victims of identity crime.

Evidence suggests that cyber-enabled identity crime is a growing threat in Australia. The Australian Institute of Criminology[4] reports that 20 per cent of Australians experienced identity crime or misuse in 2023. Additionally, 31 per cent of Australians have been affected at some point in their lives. Beyond financial damage, victims often endure substantial emotional and psychological distress. On average, individuals spend at least 13 hours addressing the consequences of identity crime.

Despite efforts to prevent and disrupt identity crime, a large number of Australians continue to be affected and require support. Demand for these support services is expected to continue to increase year on year following a 33 per cent increase from 2023-24 to 2024-25. The increasing prevalence of such crimes is placing unprecedented demand on these services.

These services remain critical for high risk and vulnerable individuals. Yet the growing scale and complexity of identity crime indicates that the current model may not be sufficient in the long term. A future-focused approach should consider how to scale support infrastructure while also empowering individuals to take greater control over their own identity protection and recovery.

To combat identity crime and protect individuals' identities, new technologies and innovative methods must be harnessed to empower individuals to safeguard their personal information. In 2022, the Australian Government established the Identity Verification Services Credential Protection Register (the Register) to disrupt identity and cybercrime, respond to data breaches, and also support and protect victims of identity crime. It is a central Register of compromised identity documents which are blocked from being used for identity verification purposes, but can still be used by an individual for their primary purpose. Since its establishment, the Register has successfully blocked 617,659 identity verification checks against compromised identity documents.

Question(s) to consider:

15. *How can support services for victims of identity crime be designed to be more effective in the context of increasing demand? How can technology be used to support individuals in managing and recovering from identity crime?*

[4] McAlister M, Faulconbridge E, Voce I and Bricknell S, Identity crime and misuse in Australia 2023, visited 3 July 2025, https://www.aic.gov.au/sites/default/files/2023-07/sb42_identity_crime_and_misuse_in_australia_2023_v2.pdf

Harmonise and simplify cyber regulation to promote best practice and efficiency

There are a number of existing regulatory schemes administered by the Australian Government and State and Territory Governments that are aimed at uplifting the cyber security of regulated entities.

For the Australian Government system, this includes regulation specifically targeted at improving the cyber security of the regulated entity. It also includes other more general regulatory obligations aimed at improving security. Some examples are set out below.

- Under the *Security of Critical Infrastructure Act 2018* (SOCI Act) specified regulated entities are required to establish, maintain and comply with a critical infrastructure risk management program that includes a process or system to comply with various standards.[5] Under the SOCI Act, Systems of National Significance may also be subject to Enhanced Cyber Security Obligations.
- A failure to adequately address cyber security risk may be a breach of company directors' duties, enforceable against directors of Australian corporations regulated by ASIC.[6]
- Under Australian Privacy Principle (APP) 11.1 under the *Privacy Act 1988* regulated entities must take reasonable steps to protect the personal information they hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure.[7] Further, under APP 11.2, regulated entities must take reasonable steps to destroy or de-identify the personal information they hold when they no longer need that information.
- *Prudential Standard CPS 234: Information Security* provides that entities regulated by the Australian Prudential Regulation Authority in the banking and insurance sectors must maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enable the continued sound operation of the entity.[8]

We have heard that Australian entities find the cyber regulatory framework complex and difficult to navigate. The Australian Government has already taken steps to address this issue through the establishment of a Single Reporting Portal on cyber.gov.au and as part of policy work being undertaken to explore options to enhance the portal and harmonise regulation.

However, there is more work to be done. As part of Horizon 2 we are exploring further options to ensure that cyber regulation is best practice and fit-for-purpose across Government. In the cyber security context, what is 'fit-for-purpose' must necessarily balance the need for the stated security outcome with the regulatory burden imposed on the entity. We want to maintain the security outcomes that the regulation is seeking to achieve, but at the lowest possible regulatory and compliance cost possible.

Getting the balance right on security regulation will ensure that Australian businesses are more secure, more productive and more competitive globally.

Question(s) to consider:

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

[5] See section 8 *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023*, https://www.legislation.gov.au/F2023L00112/latest/text

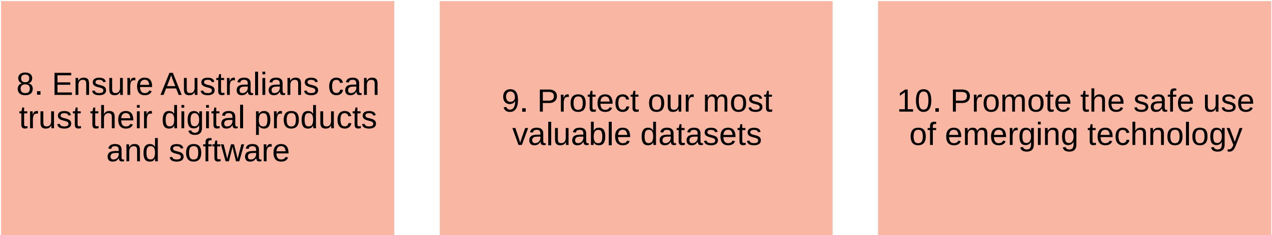
[6] Australian Securities and Investments Commission, What a Federal Court ruling on cybersecurity means for AFS licensees, accessed 27 June 2025, https://www.asic.gov.au/about-asic/news-centre/articles/what-a-federal-court-ruling-on-cybersecurity-means-for-afs-licensees/

[7] Office of the Australian Information Commissioner, Australian Privacy Principles guidelines Chapter 11: APP 11 Security of personal information, accessed 12 June 2025 (https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information)

[8] See section 15, *Prudential Standard CPS 234: Information Security*.

3.2. Shield 2: Safe technology

Under Horizon 1, we focused on setting up frameworks to lift baseline cyber security for commonly-used products and policy reviews and engagement to consider the role of data and emerging technology in Australia. There were 11 initiatives under three 'Action areas', which remain key areas of focus for Horizon 2.



8. Ensure Australians can trust their digital products and software

9. Protect our most valuable datasets

10. Promote the safe use of emerging technology

Figure 7. Shield 2 action areas for Horizon 1

Unfolding Shield 2 focus areas for Horizon 2

Ensure Australians can trust their digital products and software

Australians need to be empowered to choose to prioritise cyber security in their own digital products. However, individuals are not provided with the same choice when interacting with the connected devices implemented in our communities and infrastructure. With new devices and networks, the attack surface increases—and the consequences of unmitigated vulnerabilities can be crippling.

Edge devices

Edge devices connect Australian households and businesses to the internet. They can be hardware devices or software components, such as routers, firewalls and virtual private networks (VPNs). Edge devices act as gatekeepers between the internet and our private networks, managing and inspecting data traffic to protect the internal network. In Australia, routers enable approximately 8.3 million residential internet connections. Given that edge devices are visible from the internet, malicious cyber actors target them to gain access to an internal network's data and any connected devices. Threat actors can also use compromised edge devices as part of a botnet, a group of infected devices, to launch cyber attacks to steal data, spread malware and crash systems. As such, edge device security is critical to our broader cyber security.

Although some edge devices are covered by security standards for smart devices established under the *Cyber Security Act 2024*, further targeted intervention for edge devices may be required to provide additional protection for Australian households and businesses.

Consumer energy resources

Australia's push for renewable energy is being supported in part by consumer energy resources (CER) including rooftop solar systems, smart meters and home batteries installed on our homes. According to the Clean Energy Council, 'more than 300,000 rooftop solar systems were installed across Australia in 2024, bringing the total number to more than 4 million'.[9] While this milestone is an important component of meeting Australia's renewable energy target of 82 per cent by 2030, the internet connectivity of CER exposes the energy system to cyber threats and increases the risk of energy system disruptions. This emphasises the need for consideration of whether existing standards are adequate to protect Australian households and our energy sector from malicious actors and cyber vulnerabilities. Enabling the cyber security of CER will facilitate a secure energy system ready to support Australia's energy transition.

[9] Clean Energy Council, Clean Energy Australia Report 2025, accessed 27 June 2025, https://cleanenergycouncil.org.au/getmedia/f40cd064-1427-4b87-afb0-7e89f4e1b3b4/clean-energy-australia-report-2025.pdf

Operational technologies

Australian businesses rely on operational technologies to control and manage their industrial equipment and processes effectively and efficiently. It can be challenging to pinpoint the cyber vulnerabilities in operational technologies due to the complex and integrated structure of these technical environments.

Additionally, operational technology has unique characteristics in terms of long periods of effective life, integration across IT and IOT systems and often bespoke or business-specific functions. This makes it challenging when considering policy options to enhance security-by-design through standards.

Given the role operational technologies play in our economy, we have the opportunity to work together to determine the most appropriate approach to assure the cyber security of these devices - considering both the lessons from our domestic businesses and international partners.

Managing vendor risks

Under Horizon 2 we have the opportunity to build on previous initiatives to address foreign ownership, control and influence risks posed by technology vendors within Australia. This may include the finalisation of the *Technology Vendor Review Framework* and the public-facing Foreign Ownership, Control or Influence Risk Assessment Guidance.[10] Using a range of platforms (including the Technology Foreign Interference Taskforce)[11], we have an opportunity to look at how we engage and amplify messaging on these issues across all levels of Government, critical infrastructure, industry and Australian communities.

Question(s) to consider:

18. *What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, CER and operational technology?*

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

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

Protect our most valuable datasets

Horizon 1 initiatives, including reviews into Commonwealth data retention laws, data broker ecosystems and data sets of national significance, as well as the Government's comprehensive review of the *Privacy Act 1988*, have revealed the need to strengthen and mature Australia's data security policies.

Key findings from these reviews show that malicious actors continue to access and exploit Australian data for nefarious purposes, both through cyber attacks and legal mechanisms such as data brokers and trusted ac cess to sensitive data. Significant advancements in AI - its ability to ingest and analyse large volumes of data at scale - will enhance risks to Australian industry and communities. To keep pace, we need to enhance our data security, with a focus on how we enhance policy and regulatory frameworks, and provide greater support and guidance across industry and Government to address key risks.

The Australian Government is identifying opportunities to promote and expand the use of Digital ID in both public and private sectors, including as a mechanism to reduce the volume of personal information retained

[10] Department of Home Affairs, Foreign Ownership, Control or Influence (FOCI) Risk Assessment Guidance, accessed 27 June 2025, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/technology-and-data-security/foreign-ownership-control-or-influence-risk-assessment-guidance

[11] Department of Home Affairs, Technology Foreign Interference Taskforce, accessed 27 June 2025, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/technology-and-data-security/technology-foreign-interference-taskforce

by entities. These measures can help mitigate the risks of data breaches and identity crime, while also delivering productivity benefits through more efficient and secure identity verification processes.

Question(s) to consider:

21. *How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors?*
22. *Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed exploited by malicious actors (e.g. IP theft). How can government and industry work better together to achieve this aim in an evolving global threat environment?*

Promote the safe use of emerging technology

Technology supremacy continues to be a major driver of global strategic competition. The race for ascendancy is accelerating rapid advancements and investments in key technologies, including AI, quantum and advanced communications. While offering enormous benefits, this also has the potential to introduce new threats and harms.

The Australian Government has recently implemented several key economic and security strategies, such as the *National Quantum Strategy, Critical Infrastructure Resilience Strategy*, and *A Safer Australia - Australia's Counter-Terrorism and Violent Extremism Strategy 2025*. In Horizon 2, we will continue enabling Australians to flourish from the vast opportunities presented by digital technologies, while keeping the safety and security of our citizens, businesses and nation at the core of our approach.

Question(s) to consider:

23. *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?*

3.3. Shield 3: World-class threat sharing and blocking

Under Horizon 1 of the Strategy, Shield 3 consisted of six initiatives undertaken through two actions.

11. Create a whole-of-economy threat intelligence network

12. Scale threat blocking capabilities to stop cyber attacks

In Horizon 2, we are considering expanding the remit of Shield 3 to capture whole-of-economy cyber defence and resilience - beyond the technical solution of threat sharing and blocking. Scoping, defining and amplifying our proactive cyber security posture will be the foundation of this expansion.

Key areas of focus for Shield 3			
Encourage and enable the private sector to block threats and take a more proactive posture against cyber threat actors	**Amplify existing government and industry models for threat sharing and blocking**	**Reviewing policy frameworks as necessary for resilience to a widespread incident, conflict or crisis situations to protect Australia's national interests**	**Managing vulnerability disclosure**

Unfolding Shield 3 focus areas for Horizon 2

Encourage and enable the private sector to block threats and take a more proactive posture against cyber threat actors

Australia must adopt a proactive cyber posture to create a hostile environment for our cyber adversaries.

To deter and prevent malicious actors targeting Australia’s cyber security ecosystem, we must ensure those who are able to, are taking proactive steps to promote resilience and preparedness. We must do more to promote, clarify and support the proactive activities industry can undertake.

A good example is the work that the Council of Financial Regulators has been undertaking in partnership with industry to test the cyber defences of key organisations under the Cyber Operational Resilience Intelligence-led Exercises program (CORIE program).[12]

Question(s) to consider:

24. *What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia’s proactive cyber security posture should look like for industry?*

25. *Does the government need to provide clarity on permissible and non-permissible Active Cyber Defence in the Australian context?*

Amplify existing government and industry models for threat blocking and threat sharing

Consultation with industry and Australian Government partners during Horizon 1 identified a number of barriers and challenges to threat sharing and blocking at scale. The delivery of the National Cyber Intel Partnership (NCIP) Threat Blocking Scheme and the launch of the Cyber Threat Intelligence Sharing (CTIS) Platform by the Australian Signals Directorate during the course of Horizon 1 have addressed many of the issues that were initially identified.

To amplify and support further blocking and sharing at scale, frameworks and policy options that could be explored and co-designed with industry include:

- mapping Australia’s cyber threat intelligence sharing ecosystem to increase awareness, encourage participation, and promote threat sharing mechanisms;
- cyber threat intelligence sharing and blocking guidance for those that can share and block at scale;
- clarifying and promoting avenues to access strategic threat intelligence, and increasing strategic threat intelligence; and
- promoting and enhancing the operation of trusted groups, and if necessary expanding groups.

The focus of Horizon 1 has been on the entities that can block and share at scale (ISPs, telcos and financial services) to ensure malicious threats are blocked before they reach end users. To compliment this, under Horizon 2 we want to explore the layers of threat blocking capabilities that exist across our economy and promote the benefits of these to increase uptake (for example Enterprise Browser Security, users increasing security on browsers).

For threat sharing, under Horizon 1, the Government sought to accelerate threat sharing to establish or scale-up Information and Analysis Centres (ISACs) in low maturity sectors, focusing on the health sector. As this work continues to unfold with the creation of the Health Cyber Sharing Network (HCSN) Pilot, it will be important to monitor and evaluate how this ecosystem evolves.

Additionally, there is another intersection point with the Government’s reforms on scams. Under the *Scams Prevention Framework Act 2025* certain entities will be required to share actionable intelligence about scam

[12] Council of Financial Regulators, Cyber Operational Resilience Intelligence-led Exercises (CORIE)® Framework – July 2022, accessed 27 June 2025,https://www.cfr.gov.au/publications/policy-statements-and-other-reports/2022/revised-corie-framework-rollout/cyber-operational-resilience-intelligence-led-exercises-corie-framework.html

activity with the ACCC and/or sector regulators. The Government is now working to operationalise the intelligence sharing requirements, which will be developed and outlined in subordinate legislation.

Question(s) to consider:

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

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

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

29.How can we better align and operationalise intelligence sharing for cyber security and scams prevention?

Reviewing policy frameworks as necessary for resilience to a widespread incident, conflict or crisis situations to protect Australia’s national interests

Recent examples of crisis and conflict situations around the world have highlighted the need for both Government and industry to take an active role in working together to be prepared for cyber attacks in a time of conflict, and to have adequate frameworks in place ahead of time.

Australia recently experienced a widespread, cross-sectoral outage of digital systems through the CrowdStrike software fault in July 2024 - crashing approximately 8.5 million Windows operating systems worldwide and impacting daily life, businesses and governments across Australia and the world. The scale of the impact of the CrowdStrike incident was minimised by the company’s active cooperation with government and industry to resolve the issue. A cyber security incident of the same widespread nature as the CrowdStrike incident from an adverse actor has not yet impacted the Australian economy and has potential to be of a much larger scale due to the protracted time required to resolve.

We must ensure that Australia’s policy and legislative frameworks would enable a real-time, scalable, and sustainable response to a nationally significant cyberattack in a crisis or conflict scenario. This would require government and industry working together to explore existing frameworks, pressure-testing scenarios to identify any legislative and policy barriers, gaps and options to address them, and further consideration of legal protections to support non-government entities to block at scale.

Question(s) to consider:

30.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?

Managing vulnerability disclosure

Preventing data breaches through vulnerability disclosure is significantly cheaper than remediating a successful attack. Security vulnerability researchers notify organisations of vulnerabilities, they are a valuable, and often free resource, and would greatly enhance our cyber security resilience. However, we have heard from industry that researchers are often disengaged in Australia for a range of reasons, including the risks of being prosecuted for their actions.

The exploitation of zero-day vulnerabilities is on the rise, with 50 per cent more exploitations occurring in 2023 than in 2022. Once a zero-day vulnerability is discovered, it will be a matter of time before it becomes public knowledge, whether through the black market, or the vendor themselves notifying customers so they can take precautionary action.

From a policy perspective, more needs to be done to understand the barriers to vulnerability researchers operating in Australia, the incentives required to encourage them to operate in Australia, and incentives for in dusty to adopt vulnerability disclosure policies and utilise vulnerability researches.

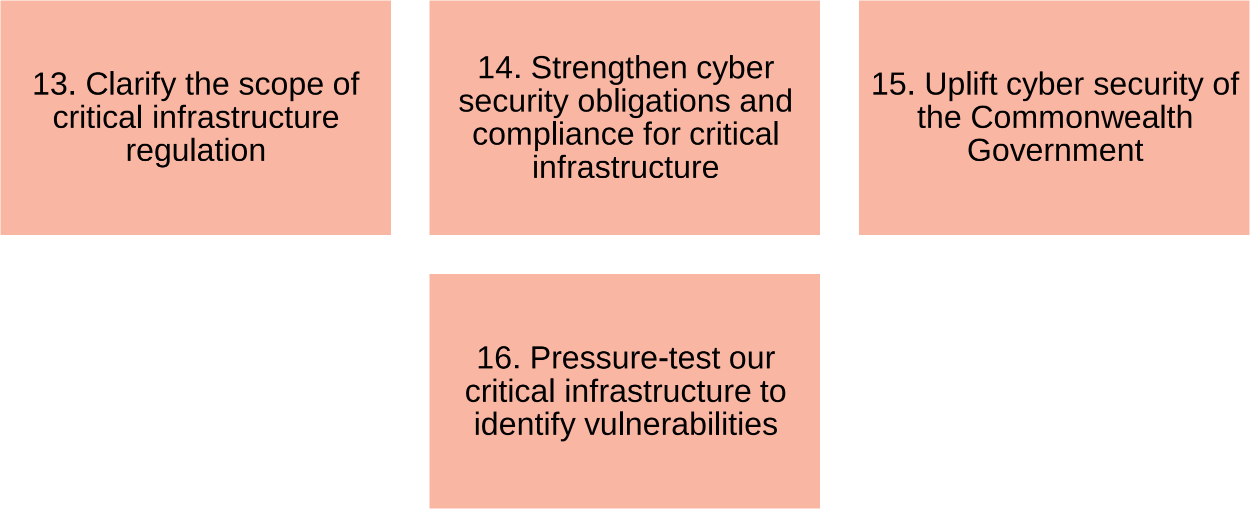
Question(s) to consider:

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

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

3.4. Shield 4: Protected critical infrastructure

Under Horizon 1 of the Strategy, Shield 4 consisted of 14 initiatives undertaken through four ‘Action areas’.



13. Clarify the scope of critical infrastructure regulation

14. Strengthen cyber security obligations and compliance for critical infrastructure

15. Uplift cyber security of the Commonwealth Government

16. Pressure-test our critical infrastructure to identify vulnerabilities

Figure 9. Shield 4 action areas for Horizon 1

For Horizon 2, we propose to build upon the successes of the four Action areas developed for Horizon 1 under Shield 4 with a particular focus on two key outcomes.

Maturation of our regulatory framework for critical infrastructure security	**Centralising cyber security risk management and prioritisation of investment and policy interventions to drive Commonwealth cyber uplift**

Unfolding Shield 4 focus areas for Horizon 2

Maturation of our regulatory framework for critical infrastructure security

Australia’s critical infrastructure plays a key role in maintaining and sustaining our economic and social stability. Unfortunately, this also makes our critical infrastructure a significant target for malicious cyber actors - as shown through the recent government advisories concerning the activities of Advanced Persistent Threat (APT) 40 and Volt Typhoon.[13,14] In Horizon 2, we expect that Government will continue to play a key role in ensuring that the cyber security of our critical infrastructure is appropriately protected and

[13] APT40 Advisory: PRC MSS in Action, Australian Signals Directorate’s Australian Cyber Security Centre, viewed 2 July 2025, https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/apt40-advisory-prc-mss-tradecraft-in-action

[14] PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, Cyber and Infrastructure Security Agency (United States of America), viewed 2 July 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

secured through regulatory schemes such as that established under the *SOCI Act 2018*.

By 2028, our aim is that Australia's critical infrastructure owners and operators will be playing a leading role in strengthening national cyber resilience, contributing to economic security and enabling ongoing trust in essential services. Cyber challenges associated with emerging technologies - such as 6G, distributed energy systems, and AI - will need to be monitored closely, and mitigated through ongoing engagement with industry and development of proportionate, risk-based policy responses.

As global interconnectivity increases, Australia will need to strengthen cooperation with international partners and the private sector in securing cross-border and shared infrastructure - particularly in areas such as undersea submarine cables and space sector assets. Government will work collaboratively with industry and international stakeholders to protect Australia's interests in a dynamic and evolving threat landscape.

Following a series of amendments in recent years, the SOCI Act now contains a world-leading legislative framework under which 'all hazards' threats to critical infrastructure, including information and cyber security threats, are regulated. This continued consolidation and refinement of the regulatory framework - including the introduction of sector specific regulations for the telecommunications sector in April 2025 - has helped to strengthen the baseline security of Australia's most important assets.

Horizon 2 provides an opportunity to continue to iterate our monitoring and enforcement framework under the SOCI Act to improve the cyber security of our critical infrastructure, supported through amendments to the regulatory scheme where necessary, through efforts such as:

- evaluating cyber security maturity levels on a sector-by-sector basis, and developing sector-specific measures and activities to increase maturity to requisite standards;
- increasing collaboration with other critical infrastructure regulators to ensure effective, efficient and right-sized regulatory activities; and
- driving increased compliance with the Critical Infrastructure Risk Management Program obligation (see Part 2B of the SOCI Act), particularly the requirement to implement a specified cyber security risk management framework, through the introduction of an independent audit requirement.

Efforts to mature our regulatory framework during the course of Horizon 2 will also be supported by outcomes from an independent review of the SOCI Act, which is expected to commence in late 2025.

Question(s) to consider:

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

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

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

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

Centralising cyber security risk management and prioritising investment and policy interventions for Commonwealth cyber security uplift to drive more coordinated outcomes

Collectively, the government is responsible for one of the largest digital estates in Australia. Essential services including emergency management, healthcare and social security all rely on this digital estate to function. Building resilience into our systems isn't just about being an exemplar, it's about protecting our way of life and vulnerable Australians who rely on government services.

By 2028, the Government will have greater visibility of technology risks across its digital estate, a data-driven and consistent approach for security assurance across the Commonwealth and the levers necessary to protect our most critical and significant systems.

In Horizon 1, the Department of Home Affairs, Australian Signals Directorate and Digital Transformation Agency have made significant progress to date in addressing known cyber security risks across Government, through investment, policy and technical advice. However, there remain a series of significant ongoing risks to the Commonwealth that includes legacy technology debt, significant requirements for further investment and the need to further professionalise entity level management of cyber security risk.

Home Affairs are considering next steps in further addressing these risks through the development of Horizon 2. The five key themes of whole-of-government Cyber Security Risk Oversight, Investment, Prioritisation, Powers, and Interventions have been developed in response to lessons from Horizon 1, following public consultation and key risk analysis.

Deliverables under Horizon 2 will be informed through information gathered in responses to the release of PSPF Directions (001-2024 Managing Foreign Ownership, Control and Influence risks, 002-2024 Technology Asset Stocktake, 003-2024 Supporting Visibility of the Cyber Threat, 001-2025 DeepSeek Products, Applications and Web Services, 002-2025 Kaspersky Lab, Inc. Products and Web Services).

Question(s) to consider:

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

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

3.5. Shield 5: Sovereign capabilities

Under Horizon 1 of the Strategy, Shield 5 consisted of four initiatives undertaken through two ‘Action areas’.

17. Grow and professionalise our national cyber workforce

18. Accelerate our local cyber industry, research and innovation

For Horizon 2, we propose to build upon the successes of the two Action areas developed for Horizon 1 under Shield 5 with a particular focus on three key outcomes.

Key areas of focus for Shield 5		
Promote a sustainable and diverse cyber workforce and business ecosystem	**Provide greater support for academic research and strengthen collaboration between academia, industry and government**	**Nurture the growth and development of robust sovereign capabilities**

Unfolding Shield 5 focus areas for Horizon 2

Promote a sustainable and diverse cyber workforce and business ecosystem

Australia’s cyber security industry supports our prosperity, generates new jobs and contributes over $2 billion to annual GDP. Since mid-2024, the Australian Government has been collaborating with cyber-focused industry leaders, academia and government agencies to explore options and ideas to promote and help build a sustainable and diverse cyber workforce in Australia.

This is a critical area of policy from a productivity perspective. According to the World Economic Forum, there is an estimated global shortage of cyber security professionals of 4 million. By 2030, that figure is expected to grow to more than 85 million workers.[15] The scarcity of cyber security professionals drives up salaries and recruitment costs, diverting resources from productive investment. In addition, where firms lack access to sufficiently skilled cyber security professionals, there can be a corresponding impact on technology adoption and digital transformation, leading to lower productivity and global competitiveness.

The Executive Cyber Council and its Cyber Workforce Working Group has taken a strong leadership role in working across industry to explore options and ideas to grow and expand Australia's skills pipeline and improve the diversity of the cyber workforce. This culminated in the inaugural *Cyber Workforce Summit* in 2024, which included over 100 participants from industry, government, industry groups and academia. The output from the Summit was the development of the Cyber Workforce Playbook, which provides a suite of actionable tools and guidance for industry to tackle cyber workforce challenges.

In addition, the Australian Government has undertaken in-depth research and engagement with key stakeholders to better understand the barriers to entry for women in the cyber workforce and potential options to support their entry and retention into the cyber workforce. There is broad agreement on the systemic challenges that limit the participation of under-represented groups, primarily misperceptions of what cyber security is, a lack of early awareness and education, the need for more inclusive workplace cultures, and better access to pathways into the field.

There is further work to do to understand what is required to support a thriving cyber workforce in Australia. For example, there is currently limited evidence to fully understand the barriers and challenges under-represented groups face entering and remaining in the cyber security sector, particularly First Nations.

There is also further work required to understand the potential for lateral skills transfer and certification simplification, and to identify sectors whose staff have transferrable skills to the cyber security sector to increase our talent pipeline. A key challenge will be understanding how Australia's cyber industry can best tap into the mid-career transitions market with transferrable skills to cyber security, and leverage industries with valuable skill sets and attributes (e.g. ability to thrive under pressure) to transfer to cyber.

Question(s) to consider:

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

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

41. 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?

Provide greater support for academic research and strengthen collaboration between academia, industry and Government

Strong partnerships are required with higher education institutions, think tanks and other government research organisations in developing cyber security policies and technologies that will underpin Australia's future digital economy.

The higher education sector plays a significant role in both the development of cyber security research and innovation, as well as the education of technical professionals who operate in the cyber workforce.

[15] World Economic Forum, Strategic Cybersecurity Talent Framework, accessed 20 June 2025, https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf

We have heard that existing collaborative efforts between academia, industry and government are segmented by design, based on agreements between individual institutions and enterprises, and often limited to short-term projects and grants. Embedding an inclusive, multidisciplinary approach to future collaboration requires a revised strategy to maximise meaningful and safe information sharing and research development. Sustainability will also be a key factors in the design of any new initiatives.

Question(s) to consider:

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

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

Nurture the growth and development of robust sovereign capabilities

Australia's cyber security ecosystem is underpinned by a range of sovereign capabilities, many of which are not seen or easily understood by the public. Some of these capabilities are niche or service a particular part of the cyber sector, but are nonetheless critical to ensuring Australia's protection and productivity. For example, data centres that host and protect critical government and industry data, or laboratories that support technical and operational elements of analysing technology for vulnerabilities. Some of these more niche sectors of the cyber sovereign capability face unique and specific challenges and require targeted interventions, or consideration in the development of broader policy ideas.

In addition, with the growing need for cyber services and workforce, industry feedback shows there is concern, at a macro level, around issues of 'concentration risk' potentially exacerbating access to services in a time of crisis or conflict. Further analysis is required in partnership between industry and government to better understand what Australian's sovereign cyber capability landscape looks like, where sovereign cyber capabilities may be required to bolster our resilience, and potential areas of vulnerability that need to be identified. This would then enable the prioritisation of sovereign capabilities for growth or development.

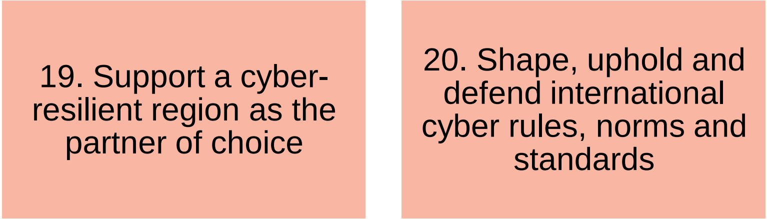
Questions to consider:

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

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

3.6. Shield 6: Strong region and global leadership

Under Horizon 1 of the Strategy, our activities under Shield 6 included eight initiatives undertaken through two 'action areas'.



19. Support a cyber-resilient region as the partner of choice

20. Shape, uphold and defend international cyber rules, norms and standards

Figure 11. Shield 6 action areas for Horizon 1

For Horizon 2, we propose to build upon the successes of the two Action areas developed for Horizon 1 under Shield 6 with a particular focus on four key outcomes.

Key areas of focus for Shield 6			
Continuing to use all arms of statecraft to deter and impose costs on state and non-state malicious cyber actors	**Strengthening cyber resilience and cooperation on critical technologies in the region and reinforcing Australia's partner of choice status**	**Continuing to shape, uphold and defend international cyber rules norms and standards in our interests**	**Driving a program of international regulatory alignment and enhancing regional cyber policy and regulatory capacity**

Unfolding Shield 6 focus areas for Horizon 2

Continuing to use all arms of statecraft to deter and impose costs on state and non-state malicious cyber actors

Australia has stepped up its efforts to raise awareness of cyber threats and impose costs to deter them. Together with international partners, we have imposed four sets of cyber sanctions on Russian cybercriminals (10 individuals and one entity) since the beginning of 2024, with discernible impact including, cost and reputational effects on the cybercriminal ecosystem. In the same time period, Australia joined or supported nine attributions of malicious cyber activity to state-based, state-backed or state-affiliated actors, including from China, Russia and Iran. We also led a technical advisory, co-sealed by Five Eyes partners, Germany, Japan and Republic of Korea which attributed malicious cyber activity to China state-backed actor APT40, and issued four statements of support for attributions made by international partners.

The attributions and advisories both damage the reputations of the states that are called out, and help raise awareness of the tactics, techniques and procedures of the malicious actors to enable community, industry critical infrastructure and government network defenders to better defend against them.

With these cyber threats set to continue to increase in Horizon 2, Australia will work to deepen collaboration with existing and additional partners on cyber deterrence, and continue efforts to build a broader coalition of international partners, including from the Pacific and Southeast Asia, willing to join in deterrence activities.

Question(s) to consider:

46. Do you view attributions, advisories and sanctions as 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?

Strengthening cyber resilience and cooperation on critical technologies in the region and reinforcing Australia's partner of choice status

Under Australia's SEA-PAC Cyber Program, the 2019-2024 Cyber and Critical Technology Cooperation Program (CCTCP) has been redesigned and refocused to achieve three specific outcomes.

1. Cyber security and critical technology capacity and capabilities are enhanced across Southeast Asia and the Pacific, including through increased access to the provision of secure and trusted technologies.
2. Cyber resilience across Southeast Asia and the Pacific is enhanced through strengthened, coordinated cyber incident preparedness and response.
3. National, regional and international cyber norms, standards, regulations and laws support an open, free and secure cyber ecosystem across Southeast Asia and the Pacific.

Stability across Southeast Asia and the Pacific is vital to Australia's security, prosperity, and national interests - as is being the partner of choice in the region. SEA-PAC Cyber builds on Australia's support to date and leverages existing partners and expertise from across the region to provide a coherent response to the cyber and critical technology challenges faced across Southeast Asia and the Pacific.

Australia has successfully established a Pacific regional cyber crisis response mechanism, Cyber RAPID, which has already been deployed ten times. We are also looking at the feasibility of a regional and scalable approach to threat blocking in the region. With increasing cybercriminal and state-sponsored malicious cyber activity in both the Pacific and Southeast Asia, demand for support on incident response, threat blocking and uplifting digital infrastructure will also increase, providing further opportunities for reinforcing our partner of choice status in the region.

Question(s) to consider:

47. Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?

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

Continuing to shape, uphold and defend international cyber rules norms and standards in our interests

In Horizon 1, Australia worked closely with international partners to protect our interests, and the interests of our regional partners, in an open, transparent, rules-based approach to the use of cyber systems, internet governance, standards development and digital trade. For example, Australia has:

- engaged in the UN Open-Ended Working Group (OEWG) on Cyber 2021-2025;
- participated in negotiations on the new UN Convention against Cybercrime, adopted by the UN General Assembly in December 2024;
- played an active role in the negotiations, including as Vice-Chair of the Ad Hoc Committee on Cybercrime (AHC) and member of the AHC Bureau;
- played a leading role in the introduction of robust provisions criminalising online child abuse and exploitation; and
- continued to work in cyber and critical technology standard setting bodies, including during the International Telecommunication Union's (ITU) World Telecommunication Standardization Assembly 2024 (WTSA-24).

Australia continues to work with international partners on internet governance, with a focus in our region, to ensure the existing model in which government, industry, the technical community, academia and civil society work together to preserve an open, secure, interoperable and free global internet is preserved.

Question(s) to consider:

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

Driving a program of international regulatory alignment and enhancing regional cyber policy and regulatory capacity

The global cyber threat environment is escalating in both complexity and frequency, with malicious cyber actors exploiting regulatory fragmentation across jurisdictions. In response, many leading economies have a dvanced their cyber security regulatory frameworks, introducing mandatory reporting and strong enforcement regimes. As a result, we have heard from industry that divergent cyber regulations across international jurisdictions are placing increasing strain on businesses and national coordination efforts alike.

Australia has made important developments through the Strategy to enhance alignment of regulation in our domestic setting. However, in an increasingly interconnected digital world, Australia's cyber regulatory framework has a valuable opportunity to draw lessons from leading global peers such as the EU, UK, US, Canada and Singapore, to work together to consider opportunities for greater regulatory alignment.

Question(s) to consider:

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