Australian Government

2023–2030 Australian Cyber Security Strategy

© Commonwealth of Australia 2023

With the exception of the Commonwealth Coat of Arms, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license at https://creativecommons.org/licenses/by/4.0/legalcode.

This means this license only applies to material as set out in this document.

The details of the relevant license conditions are available on the Creative Commons website at https://creativecommons.org/ as is the full legal code for the CC BY 4.0 license at https://creativecommons.org/licenses/by/4.0/legalcode.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed at the Department of the Prime Minister and Cabinet website— https://www.pmc.gov.au/government/commonwealth-coat-arms.

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

P - 23-02503-a

2023–2030 Australian Cyber Security Strategy

Contents

Minister's foreword 4

Executive summary: Our 2030 Vision 6

Strategic context 11

Why we must act now 12

Why Australia has an opportunity to lead 13

Our Strategy 15

Shield 1: Strong businesses and citizens 16

1. Support small and medium businesses to strengthen their cyber security 18
2. Help Australians defend themselves from cyber threats 19
3. Disrupt and deter cyber threat actors from attacking Australia 20
4. Work with industry to break the ransomware business model 22
5. Provide clear cyber guidance for businesses 23
6. Make it easier for Australian businesses to access advice and support after a cyber incident 25
7. Secure our identities and provide better support to victims of identity theft 26

Shield 2: Safe technology 28

8. Ensure Australians can trust their digital products and software 29
9. Protect our most valuable datasets 31
10. Promote the safe use of emerging technology 32

Shield 3: World-class threat sharing and blocking 34

11. Create a whole-of-economy threat intelligence network 35
12. Scale threat blocking capabilities to stop cyber attacks 37

Shield 4: Protected critical infrastructure 38

13. Clarify the scope of critical infrastructure regulation 40
14. Strengthen cyber security obligations and compliance for critical infrastructure 41
15. Uplift cyber security of the Commonwealth Government 42
16. Pressure-test our critical infrastructure to identify vulnerabilities 44

Shield 5: Sovereign capabilities 46

17. Grow and professionalise our national cyber workforce 47
18. Accelerate our local cyber industry, research and innovation 50

Shield 6: Resilient region and global leadership 52

19. Support a cyber resilient region as the partner of choice 53
20. Shape, uphold and defend international cyber rules, norms and standards 55

Next steps: Implementation and evaluation 57

How we will ensure we are on track to deliver 57

Appendix A: List of acronyms 59

Minister's foreword

The Hon Clare O'Neil MP

Minister for Home Affairs | Minister for Cyber Security

Cyber security is an urgent national problem, and we need to act now. After a decade of malaise, Australia has fallen behind. For too long, Australian citizens and businesses have been left to fend for themselves against global cyber threats.

Cyber security touches the lives of every Australian. Over the past 18 months, millions of Australians have been affected by devastating cyber incidents. On average, one cybercrime is reported every 6 minutes, with ransomware alone causing up to $3 billion in damages to the Australian economy every year[1].

And, we have good reasons to believe that the threat is going to continue to grow. Artificial intelligence and machine learning will bring new kinds of risk. The Internet of Things will lead to billions of additional devices being connected to the Internet, opening new scope for cyberattack. And, our geopolitical environment is the most challenging we have faced since the Second World War.

We must not forget that cyber security is also a big opportunity for our country. The global cyber industry is massive and it is growing rapidly, and it is here to stay. If we play it right, Australia is uniquely placed to create well-paid jobs for Australians and products that we can export all over the world.

Over the last 12 months, I have engaged hundreds of business leaders, community representatives and cyber experts within Australia and from around the world. I have stepped into the security operations centres of some of the biggest Australian companies. I have spoken with small business owners, universities, not-for-profits, and community leaders.

The one thing I have heard consistently is that Australians are demanding action on cyber. It is time for real and meaningful change. That's why the Albanese Labor Government is launching the *2023-2030 Australian Cyber Security Strategy*. This Strategy sets out our bold vision for Australia to be a world leader in cyber security by 2030.

Our Strategy will change the game for Australia's cyber security. Under the Strategy, we are building six 'cyber shields' to help defend our citizens and businesses from cyber threats. Each shield provides an additional layer of defence, making Australia a harder target.

But we're not only reinforcing our defences. We're also investing in national cyber resilience, so we can bounce back when we get hit. And we're fighting back, deploying Australia's leading cyber capabilities to put malicious actors on notice. We are rallying our international network of cyber guns to help break the business model of ransomware and cybercrime.

1. ASD (2023). ASD Cyber Threat Report 2022–2023.

Our Strategy calls for a new era of collaboration on cyber in Australia. We're leading by example, producing a strategy that defines a clear vision for both domestic and international cyber security for the first time.

We want to remain the security partner of choice for nations in the Pacific family. We've consulted closely with our regional partners to understand their unique cyber challenges. We've heard from Pacific Islands that digitisation and connectivity are key parts of their economic development strategies, but also increase the cyber risks they face as nations.

Consultation is at the heart of this Strategy. Input from thousands of experts, businesses and citizens across nearly every sector of the economy have contributed to this plan.

In December 2022, I appointed an Expert Advisory Board to guide the development of the Strategy – chaired by Andrew Penn AO, former CEO of Telstra, with Rachael Falk, CEO of the Cyber Security Cooperative Research Centre, and Mel Hupfeld AO DSC. The Board authored a Discussion Paper which received over 330 written responses. I am deeply grateful for the stewardship of the Board, and for their immense contribution to the Strategy.

Cyber security requires government and big business to lead. From today, we are shifting more of the cyber risk to those who are most capable. We are holding industry to higher standards to protect our devices, our data, and our critical infrastructure. For the first time, Government will hold itself to the same standard it expects of industry.

The strategy is bold and ambitious – and it has to be. Because one thing is abundantly clear from what's happened to our cyber environment in the last five years: we simply can't continue as we are. We need to push harder, we need to get in front of this problem, and for the first time, Australia's Cyber Security Strategy will help our country do just that.

The Hon Clare O'Neil MP
Minister for Home Affairs and Cyber Security

Executive summary: Our 2030 Vision

By 2030, Australia will be a world leader in cyber security.

We envisage a future where stronger cyber defences enable our citizens and businesses to prosper, and to bounce back quickly following a cyber attack.

To achieve our vision, we need to protect Australians. We will do this with six cyber shields.

Each shield provides an additional layer of defence against cyber threats and places Australian citizens and businesses at its core. Throughout the period covered by the *2023–2030 Australian Cyber Security Strategy* (the Strategy), the Australian Government will work with industry to reinforce these shields and build our national cyber resilience.

Figure 1: Cyber shields

Our cyber shields

1

Strong businesses and citizens

Our citizens and businesses are better protected from cyber threats, and can recover quickly following a cyber attack.

2

Safe technology

Australians can trust that their digital products and services are safe, secure and fit for purpose.

3

World-class threat sharing and blocking

Australia has access to real-time threat data, and we can block threats at scale.

4

Protected critical infrastructure

Our critical infrastructure and essential government systems can withstand and bounce back from cyber attacks.

5

Sovereign capabilities

Australia has a flourishing cyber industry, enabled by a diverse and professional cyber workforce.

6

Resilient region and global leadership

Australia's region is more cyber resilient, and will prosper from the digital economy. We will continue to uphold international law and norms and shape global rules and standards in line with our shared interests.

We need to act now.

Cyber security touches the lives of every person in the country. Australia is an attractive target for cyber criminals; over the past year, millions of Australians have had their personal data stolen and released online. Emerging technology is changing our digital landscape, with the rise of artificial intelligence (AI) and quantum computing creating new opportunities and challenges for cyber security. The stakes in protecting our people and businesses have never been higher.

Cyber security presents rich opportunities for Australia.

Cyber security is not just about defending ourselves against threats – it's critical to support the rapid adoption of new technologies, boosting productivity and growing the digital economy. Cyber security presents a thriving and growing business opportunity for our country. An investment in our cyber security is an investment in our economic security. If we act quickly, Australia can take advantage of the opportunity to turbocharge our tech sector and create prosperity for our citizens. We can become a global leader in cyber technologies and be recognised as a top destination of choice for cyber talent. Our strategy will put Australia in the fast lane for cyber research, innovation, and entrepreneurship. By 2030, Australia can lead the cyber frontier.

Australia is uniquely placed to capture this opportunity.

Although there's a lot of work to do, we are starting from a position of strength. Australia has an extensive track record of trailblazing legislative reform. From our workplace health and safety reforms to our tobacco plain packaging laws, Australia has continuously set global standards for public safety. But regulation is not the only solution – we've also got strong cyber offensive capabilities, led by the Australian Signals Directorate (ASD) and the Australian Federal Police (AFP). Our world-class research and education institutions will allow Australia to become a global leader in cyber innovation. Our tech sector is growing rapidly, enabled by the Government's once-in-a-generation reform of the migration system. We're supported by our deep and trusted partnerships across the globe, including strong relationships with our regional neighbours, Quad and Five Eyes partners.

We will deliver our strategy across three horizons.

The journey to achieve our 2030 vision requires multiple phases of work and ongoing collaboration between the Government and industry to uplift our cyber maturity. We will deliver our strategy in three phases:

- **In Horizon 1 (2023–25):** we will strengthen our foundations. We will address critical gaps in our cyber shields, build better protections for our most vulnerable citizens and businesses, and support improved cyber maturity uplift across our region.
- **In Horizon 2 (2026–28):** we will scale cyber maturity across the whole economy. We will make further investments in the broader cyber ecosystem, continuing to scale up our cyber industry and grow a diverse cyber workforce.
- **In Horizon 3 (2029–30):** we will advance the global frontier of cyber security. We will lead the development of emerging cyber technologies capable of adapting to new risks and opportunities across the cyber landscape.

We have a clear roadmap for delivery.

Alongside the Strategy, we are releasing an Action Plan that outlines the initiatives that we will deliver in Horizon 1. The Action Plan details immediate actions that we will take as our first steps on the journey towards our 2030 vision. It defines clear accountabilities for each initiative, identifying lead and supporting agencies. To ensure that we remain on track, the Government will continue to evaluate our progress and adjust our plan in response to new threats or emerging technologies.

We will continue to engage with industry at every step.

As part of Horizon 1, Government will work with industry to co-design a suite of landmark legislative reforms that will help us strengthen our cyber shields. This will include options for new cyber obligations, streamlined reporting processes, improved incident response and better sharing of lessons learned after a cyber incident. This package will be designed with careful consideration to minimise regulatory burden. As we want our laws to reflect expert advice and consider the needs of all Australians, we are kicking off a targeted co-design process before these changes are made.

Our vision is bold and ambitious, but we have a plan to get there.

Australians deserve gold-standard cyber defences and access to the vast economic opportunities that a strong cyber posture presents. This Strategy marks a significant shift in Australia's approach to protecting our people and businesses from cyber threats. By building and strengthening our cyber shields, Australians will work together to secure a safe and prosperous digital future. This Strategy charts our course to get there.

Strategic context

Strategic context

The cyber landscape is evolving quickly, but Australia has a unique opportunity to lead.

Today, Australia faces a complex cyber security landscape. Australia's economy is digital, and the continued adoption of safe and secure digital platforms, technologies and online services is critical for our nation's productivity and future prosperity. However, cyber attacks are growing in number, speed and sophistication. The stakes are higher than ever before, with our most sensitive data and most vulnerable members of the community at risk. But we also have a unique opportunity to become a global leader in cyber security.

Why we must act now

Cyber attacks are accelerating faster than ever before, and we can't afford to wait any longer. Malicious activity targeting Australians through cyberspace continues to grow at an unprecedented rate, with cybercriminals and state-based or state-sponsored actors routinely targeting our networks and data. The industrialisation of cybercrime has made it easier than ever for malicious actors to steal valuable data, disrupt our systems and extort Australians for financial gain. Capabilities and skills that were once solely the domain of states are now available for purchase and hire by state and non-state groups. State-sponsored actors continue to use cyber operations to steal information and challenge our sovereignty. Criminals and states not only seek to exploit vulnerabilities in our devices and people, but also disrupt critical infrastructure and government systems.

As malicious actors grow in number, they are also taking advantage of more advanced tools. Critical and emerging technologies such as AI, quantum computing and biotechnology will revolutionise every aspect of Australian life. They will create economic and commercial opportunities, improve the provision of government services, and enable better health outcomes. However, these technologies will also create new opportunities for malicious cyber actors. As our networks and systems become increasingly interconnected, our attack surface will expand, allowing malicious actors greater opportunity to target Australians with scale and speed. Data that is safe today may not be tomorrow.

Failing to defend our country from cyber attacks will have devastating impacts on our society and digital economy. As a prosperous country with high online connectivity, Australia is a very attractive and profitable target for cybercriminals. Ransomware, cyber extortion, scams and digital theft all take a significant toll on Australian businesses and the community. The cost of cybercrime on Australian businesses is growing by up to 14% per annum [2].

2. ASD (2023). ASD Cyber Threat Report 2022–2023.

Why Australia has an opportunity to lead

Australia is not starting from scratch. We have a solid foundation on which to become a world leader in cyber security. It is on this foundation that we have built our Strategy.

One of Australia's core strengths is our robust legislative system. Our strong legislative and regulatory frameworks will help enforce new cyber security standards, while our ability to quickly change these laws will help us adapt to meet our evolving cyber security needs. From regulation of critical infrastructure under the *Security of Critical Infrastructure Act 2018* (the SOCI Act) to the protection of people, information and assets in the Australian Government under the *Protective Security Policy Framework* and associated state and territory arrangements, the Australian Government can access a suite of levers to enhance our national cyber security. We are well placed to enact further legislative reform to achieve real whole-of-society changes.

Not only do we have strong laws, we also have strong defences. Australia has a wide range of intelligence, defensive and offensive cyber capabilities to respond to serious cyber attacks. The ASD works across the full spectrum of cyber operations to defend Australia from global threats and advance our national interests. ASD acquires signals intelligence, provides proactive cyber risk advice and assistance, and may deploy offensive cyber operations. These operations are designed to deter, disrupt, degrade and deny adversaries where consistent with ASD's existing legislative and oversight framework, in addition to domestic and international law. The AFP leads the investigation of serious and organised cybercrime activity impacting government, systems of national significance, or the wider Australian economy.

The capabilities of ASD and AFP are also enabled by many other government agencies, industry leaders and community groups. This includes our world-class research, education and tech sectors, which are driving major technological advancements in cyber security and adjacent fields. Australia has many globally successful technology companies and strong research capabilities in critical technologies, including quantum, robotics and AI. Deep partnerships between academia, industry and government mean that we can afford to raise our aspirations about what Australia can achieve.

In our region, Australia is a trusted partner of choice. We place great value on a strong region and collective capacity building. We have strengthened cyber resilience in our region by supporting the establishment of national computer emergency response teams, assisting in the development of new or strengthened national cyber strategies and legislation, delivering awareness-raising campaigns promoting online safety, and advocating for global tech companies to take security and safety more seriously.

Globally, Australia is a leading voice on cyber security. Through multilateral forums, we have demonstrated a long-standing commitment to upholding the rules-based international order. We have stood up for responsible state behaviour in cyberspace and called out instances of malicious cyber activity by nation states. As a trusted voice on the international stage, Australia has an opportunity to uplift global standards for cyber security.

These strengths are the backbone of our Strategy, and they fuel our vision for a more secure future. By building on our strategic advantages and capturing new opportunities, Australia can become a world leader in cyber security by 2030.

Our Strategy

Shield 1

Strong businesses and citizens

Our citizens and businesses are better protected from cyber threats, and can bounce back quickly following a cyber attack.

What success looks like

In 2030, all Australians will benefit from a strong digital economy. We envision a future where every individual and business has the skills and resources they need to be cyber secure.

Cyber is no longer a technical topic but a whole-of-nation effort. Responsibility for cyber security is shared across the community, with more cyber risk allocated to those who are most capable of addressing them. Small businesses and vulnerable groups will have dedicated support from government and industry. Government will help business leaders understand their cyber maturity and find ways to embrace digital technology while continuing to protect their customers. Diverse communities – including remote and regional communities, culturally and linguistically diverse groups, First Nations communities, young people, seniors, people with disabilities, and neuro-diverse people – will be empowered to build their cyber resilience. Australians will have a clear understanding of cyber risks and know how to get help quickly.

By 2030, Australia will be a hard target for cyber attacks. Our objective is to undermine cybercrime business models and put Australians in a strong position to respond effectively, including if they are asked to pay a ransom. Larger businesses will play a central role in strengthening the security of the economy by helping to protect those less able to do so. If cyber extortion occurs, Australians will know how to respond safely.

Cyber incidents are inevitable; it's a part of life and doing business online. Yet if things go wrong, the Australian Government and our community will be well prepared to work together and bounce back swiftly. The National Cyber Security Coordinator (Cyber Coordinator) and the National Office of Cyber Security will coordinate whole-of-government incident response efforts. Businesses will find it easier to report cyber incidents and victims of cybercrimes will get the support they need to recover.

How we'll get there

To achieve our 2030 vision, the Australian Government will:

- support small and medium businesses to strengthen their cyber security;
- help Australians defend themselves from cyber threats;
- disrupt and deter cyber threat actors from attacking Australia;
- work with industry to break the ransomware business model;
- provide clear cyber guidance for businesses;
- make it easier for businesses to access advice and support after a cyber incident; and
- secure our identities and provide better support to victims of identity theft.

1 Support small and medium businesses to strengthen their cyber security

The problem we face

Small and medium businesses play a vital role in our economy, contributing more than $500 billion[3] to annual gross domestic product and employing around 43% of the private sector labour market.[4] But Australian small businesses consistently express concern over their lack of time, resources and expertise to uplift their cyber security. They struggle to attract and retain skilled cyber professionals, procure the right services or know where to invest in uplifting their cyber resilience. As a consequence, small and medium businesses can take longer to recover from a cyber incident and face higher costs compared to larger businesses.

For large organisations, incidents affecting a small or medium business in their supply chain can cause significant damage. An incident in a large organisation's supply chain can cause major downstream impacts, disrupting service delivery. Or, where a small business is integrated into the networks of a large organisation, a cyber attack on the smaller entity can unlock a 'back door' into the larger organisation that malicious actors can easily exploit.

How the Government will take action

The Australian Government recognises that uplifting cyber maturity can be challenging for small and medium businesses, particularly when balancing competing priorities. Without appropriate support and guidance, investment in cyber security can seem overwhelming.

Under this initiative, the Government will:

1. Offer advice and guidance to support small and medium businesses

The Government will create a **cyber health-check program** that will offer a free, tailored assessment of cyber security maturity to small and medium businesses. Based on international exemplars, the health-check program will provide educational tools and materials to help small and medium businesses improve their cyber security posture.

The health check program will support the delivery of the existing Cyber Wardens Program for small businesses, which allows them to better understand cyber security risks and build in house capability to manage cyber threats.

As cyber security requirements for small and medium businesses evolve, the Government will continue to adapt its guidance for business leaders. The Government will ensure that small business support programs are easy to understand and accessible, and that businesses have strong incentives to participate. Wherever possible, the Government will limit regulatory burden on small businesses and help them to do what they do best: focus on their businesses and the goods and services they provide.

3. Australian Small Business and Family Enterprise Ombudsman (2023). Small Business Matters.
4. Reserve Bank of Australia (2023). Recent Developments in Small Business Finance and Economic Conditions.

2. Build cyber resilience and provide support when an incident occurs

The Government will continue to provide victim support services for small businesses to help them respond to cyber incidents and bounce back quickly. These services will be closely coordinated with other support for small businesses, including anti-scams programs led by the National Anti-Scam Centre.

The Government's new **Small Business Cyber Security Resilience Service** will provide small businesses with advice on how to build their cyber security capability and resilience. This 'one-stop-shop' will also help small businesses deal with the aftermath of a cyber incident and recover quickly. Staffed by professionals who understand small business, cyber security and mental health, this service will provide small businesses with assistance that is tailored to their situation, capability and level of cyber risk.

2 Help Australians defend themselves from cyber threats

The problem we face

We must do more to lift cyber awareness across our community. It can be difficult to understand how to protect ourselves online and for many Australians, good cyber security behaviours are not front of mind. Yet much like washing our hands or putting on our seatbelts, cyber security needs to become part of our everyday routine. It's important to emphasise that basic actions – like maintaining a secure pass-phrase, keeping our software up to date, or not clicking on suspicious links – can have the most effective outcomes.

The landscape of cyber security advice remains hard to navigate for many Australians, particularly for diverse communities who may be more vulnerable to cyber incidents and cybercrime. Further collaborative and coordinated action between government, business and civil society is necessary to simplify the way we talk about cyber security and emphasise that secure cyber practices can be an everyday skill.

How the Government will take action

Building cyber awareness will provide Australians with confidence and trust to embrace digital technologies and the opportunities they present. The Australian Government recognises that genuine behavioural change will take time and is committed to delivering awareness-raising programs over the long term.

Under this initiative, the Government will:

1. Extend the reach and accessibility of cyber awareness programs

The Government will continue the **national cyber awareness campaign** to help Australians understand critical cyber security threats and how to protect themselves online. Partnerships with the private sector and civil society will be critical to extend the reach of this national campaign and maintain consistent messaging. The Government will also coordinate this work with other related areas – such as scams, fraud, identity resilience and Digital ID – to uplift consumer awareness against online threats across the board.

2. Empower vulnerable communities to grow their cyber literacy

The Government will **empower community organisations** to deliver tailored cyber awareness campaigns to diverse groups, funded by a community grant program. This program will allow local community leaders to tailor cyber awareness campaigns to the unique needs of diverse cohorts – such as remote and regional communities, culturally and linguistically diverse groups, First Nations communities, young people, seniors, people with disability and neuro-diverse people. Through this program, Government will collaborate with community leaders to develop bespoke strategies and materials to more effectively engage these groups. This program will be coordinated with other awareness campaigns, such as on scams, to ensure that these communities receive clear and consistent advice.

3 Disrupt and deter cyber threat actors from attacking Australia

The problem we face

Cybercrime, including ransomware and cyber extortion, can cause large-scale harm to the Australian economy and national security. Cyberspace is borderless: malicious state actors and cybercriminals can compromise systems and technologies at distance and at scale. Such attacks often require minimal technical expertise and few resources, yet can have a major impact – potentially crippling core business functions and critical services like our telecommunication networks, health system, food supply chains and educational institutions.

Cybercrime is causing significant disruption to our economy. From mid-2022 to mid-2023, the cost of cybercrime for Australian businesses rose by 14%. The average cost of cybercrime for small businesses is now $46,000; $97,200 for medium businesses; and $71,600 for large businesses.[5] These cyber attacks on our businesses, democratic institutions and critical infrastructure are unacceptable. Rules and law apply online, just as they do offline.

How the Government will take action

The Australian Government recognises the significant impact cybercrime can have on individuals. Responsibility for cyber deterrence should sit with those most capable of taking defensive action, so the Government will use all lawful and appropriate levers to deter and disrupt cybercrime.

Under this initiative, the Government will:

1. Build our law enforcement and offensive capabilities

We will amplify our domestic law enforcement and offensive cyber activities to make Australia a harder target for cyber criminals. We approach this task from a position of strength: Australia is considered a world leader in our investigatory powers and criminalisation frameworks to combat cybercrime.

5. ASD (2023). ASD Cyber Threat Report 2022–2023.

The Government will expand the AFP's contribution to **Operation Aquila**, the AFP- and ASD-led joint standing operation aimed at investigating and disrupting criminal syndicates. Through Operation Aquila, the AFP and ASD use offensive cyber capability as a criminal investigation tool towards prosecution or disruption. Operation Aquila focuses on the highest-priority cybercrime threats impacting Australia, both nationally and internationally. New funding for Operation Aquila will enhance the AFP's offensive cyber capability to investigate and disrupt cybercrime activity.

The Government is also continuing to deliver ASD's **Project REDSPICE** to build world-class, innovative offensive cyber capabilities that can deliver real world impact to deter, disrupt, degrade and deny cybercrime. Project REDSPICE will triple Australia's offensive cyber capabilities and put malicious threat actors on notice. While details of specific offensive cyber capabilities and operations remain classified, we are committed to transparency about the rights and obligations that govern their use.

2. Shape international legal frameworks and cooperation on cybercrime

Cybercrime is a global threat that requires global solutions. Deepening international collaboration is essential to combat the transnational threat of cybercrime.

The Government will continue to **drive global cooperation to effectively prevent, deter and respond to cybercrime**. We will continue to work with our international partners to crack down on cyber criminals, including close collaboration with the Five Eyes and international law enforcement partners via our existing network of AFP liaison officers. We will continue to advocate for global legal frameworks that effectively combat cybercrime in addition to frameworks that protect human rights, fundamental freedoms and the rule of law. This includes supporting global efforts to adopt and implement the Council of Europe Budapest Convention on cybercrime.

In collaboration with our global partners, we will seek to hold criminal groups accountable for their actions. We will also seek to hold states accountable for malicious cyber activity perpetrated by actors given safe haven in their territories. We will impose a cost on those responsible for cyber incidents, including making public attributions and imposing sanctions when we have sufficient evidence and it is in our national interests to do so.

We will also **build regional capabilities to fight cybercrime** in the Pacific and Southeast Asia, through forums such as the Pacific Islands Law Officers' Network and ASEAN Senior Officials Meeting on Transnational Crime. To protect our shared interests, Government will continue to support more countries within our region to shape the development of new and emerging international legal frameworks on cybercrime.

4 Work with industry to break the ransomware business model

The problem we face

Ransomware is one of the most disruptive cyber threats in the world today. Ransomware and cyber extortion attacks have demonstrated their capacity to disrupt the lives and livelihoods of Australians. Malicious cyber actors are developing new technologies to automate ransomware attacks. 'Ransomware-as-a-service' products can be purchased on the dark web, making it easier than ever for criminals to steal valuable data.

Ransomware incidents are under-reported, limiting our national understanding of their true impact on the economy. Reduced visibility of ransomware attacks can impact incident response and harm mitigation efforts. Poor visibility of threats may also contribute to underdeveloped business risk models.

The ransomware business model is fuelled by payments made to cybercriminals, with cryptocurrency transactions enabling malicious actors to anonymously profit from extortion claims. Paying a ransom does not guarantee that sensitive data will be recovered. It also makes Australia a more attractive target for criminal groups.

Throughout consultation, we have heard that businesses feel alone when tackling ransomware. Business leaders do not have clear guidance on how to prevent and respond to cyber extortion.

How the Government will take action

To make Australia a hard target for ransomware, we must disrupt the ransomware business model. The Australian Government will take strong action to prevent cybercriminals from profiting from attacks on Australian citizens and businesses.

Under this initiative, the Government will:

1. Enhance visibility of the ransomware threat

We need early warnings of ransomware attacks to enable the Government to provide the right support at the right time. We also need to build an improved picture of the ransomware threat so that we can develop appropriate responses. To stay ahead of the threat, we will co-design with industry options to legislate a **no-fault, no-liability ransomware reporting obligation** for businesses.

Pending design, anonymised reports of ransomware and cyber extortion trends could be shared with industry and the broader community to help us take steps to build our national resilience against cybercrime.

2. Provide clear guidance on how to respond to ransomware

Consistent with our **Counter Ransomware Initiative** (CRI) commitment, the Australian Government continues to strongly discourage businesses and individuals from paying ransoms to cybercriminals. There is no guarantee you will regain access to your information, or prevent it from being sold or leaked online. You may also be targeted by another attack.

We've consistently heard that Australian businesses and citizens need clearer advice on how to respond to ransom demands. As a next step, the Government will **build a ransomware playbook**. This playbook will provide clear guidance to businesses and citizens on how to prepare for, deal with, and bounce back from ransom demands.

3. Drive global counter-ransomware operations

We will continue to work with our international partners to drive the CRI and **lead global cooperation** to break the ransomware business model. Australia will take a leadership role to drive international action to fight back against the threat, starting with our role as Chair of the International Counter Ransomware Taskforce. Under the CRI, we are working with 50 international partners to execute counter-ransomware operations. The Australian Government will continue working with CRI members to strongly discourage anyone from paying a ransomware demand.

The Government will also continue its efforts to regulate the use of cryptocurrencies. The Attorney-General's Department is consulting on major reforms of Australia's anti-money laundering and counter-terrorism financing laws, including their application to transactions involving digital currencies. Separately, the Department of the Treasury is consulting industry on defining digital asset types and seeking to identify gaps in the current regulatory framework in relation to digital currencies.

5 Provide clear cyber guidance for businesses

The problem we face

Cyber security is not just good practice; it's good business. A clear understanding of how to manage cyber risks is essential for Australian businesses embracing the digital economy. Many cyber risks could be mitigated by better corporate governance from the board down.

Businesses already have existing obligations to protect their businesses from risk. These obligations include protecting their businesses and customers from cyber attacks. But many expectations of cyber governance are unclear, and there is scope to identify gaps in the current suite of cyber obligations. Industry feedback has flagged that more could be done to help businesses understand what good cyber security looks like.

When a major incident occurs, it is important that we understand the vulnerabilities that led to the malicious attack – and share lessons learned with industry to enhance future cyber readiness. The Government must enable the efficient and well-targeted delivery of appropriate guidance to industry to ensure identified vulnerabilities are not further exploited.

How the Government will take action

The Australian Government will work with industry to ensure cyber security is appropriately considered in the boardroom, informed by clear guidance on cyber best-practice and lessons learned from previous cyber incidents.

Under this initiative, the Government will:

1. Clarify business expectations of cyber governance

The Government will consider how best to provide additional information on **cyber security guidance for businesses** to help them navigate important obligations and requirements that should be considered when developing cyber security frameworks. As a first step, the Government will publish an overview of corporate obligations for critical infrastructure owners and operators. Next, the Government will consider how best to collaborate with industry to design best-practice principles to guide good cyber governance.

Initiatives in this space would aim to be principles-based, technology neutral and applicable to a range of organisations, regardless of their cyber maturity. It will build on existing resources available through the Australian Institute of Company Directors, Australian Information Security Association, Australian Securities and Investments Commission, ASD's Australian Cyber Security Centre (ACSC), the National Anti-Scam Centre, and the Cyber Security Cooperative Research Centre.

2. Share lessons learned from cyber incidents

The Government will establish a new process for conducting lessons-learned reviews of significant cyber incidents. We will work with industry to establish a new **Cyber Incident Review Board**, drawing on international and domestic models, including the United States Cyber Safety Review Board and the Australian Transport Safety Bureau.

Following major cyber incidents, this no-fault post-incident review mechanism will seek to uplift collective cyber security, boosting our ability to hone incident preparation and response. The proposed review mechanism will not make findings of fault and will not interfere with incident response or regulatory, intelligence or law enforcement functions.

Lessons learned from these reviews will be shared with the business community and the wider public. Insights on cyber best-practice will be fed into our national threat intelligence sharing and blocking networks, our cyber awareness programs, national cyber exercises and other initiatives to continue to improve our national cyber resilience.

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

The problem we face

When a cyber incident occurs, every moment matters. Rapid response will increase the chances of timely recovery and help Australian businesses bounce back quickly. However, industry have flagged barriers that make it challenging to get help after a cyber incident.

Australia's current regulatory reporting requirements for cyber incidents are complex. Businesses often need to report an incident to multiple regulators, depending on their sector, the nature of the incident, and the severity of the consequences. These obligations serve an important purpose, but they must not hinder the capacity of business leaders to respond to an incident.

Additionally, industry are increasingly reluctant to share detailed and timely cyber incident information with ASD. Businesses are concerned that the information they share could be used for regulatory action. Such reluctance can limit the Government's capacity to offer support during an incident, and it reduces our understanding of the national threat picture.

Industry has also flagged difficulties when engaging incident response firms. There is lack of clarity around professional standards for incident response providers, leading to inconsistent service quality. Without rapid and high-quality support, incidents can grow in scale and cause devastating consequences for Australian businesses and citizens.

How the Government will take action

The Australian Government has already taken steps by appointing the Cyber Coordinator to lead the coordination and triaging of government action in response to a major cyber incident. Building on this, the Government will put measures in place to ensure industry is supported as effectively as possible during a cyber incident.

Under this initiative, the Government will:

1. Simplify incident reporting

Through Project REDSPICE, the Government is already enhancing cyber security incident reporting through its one-stop shop at cyber.gov.au. To help industry navigate mandatory cyber incident reporting obligations, the Government has developed a **single reporting portal** on cyber.gov.au that brings key reporting links together in one place.

As a next step, the Government will explore options to make it easier for businesses to meet their regulatory obligations, which may include potential regulatory change or form simplification.

2. Promote access to trusted support after an incident

Information provided to Government in the early stages of a cyber incident is critical to effective incident response. We will encourage open engagement with Government during an incident by co-designing options to legislate a **limited use obligation for ASD and the Cyber Coordinator**. This obligation would aim to limit how information that industry shares with ASD and the Coordinator can be used by other Australian Government entities, including regulators. A limited use obligation would not impact regulatory or law enforcement actions, or provide an immunity from legal liability. As an immediate step, we will start by developing an interim approach for ASD.

The Government also seeks to provide business and community leaders with greater confidence when they engage cyber security professionals. This will include co-designing an **industry code of practice for incident response providers**. This code will clearly define the service quality and professional standards that are expected from third-party cyber incident response providers. This code will be co-designed with industry to ensure that cyber security firms provide fit-for-purpose services consistent with public expectations.

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

The problem we face

Our identities are one of the most sensitive and valuable types of personal data. Cybercriminals go to great lengths to steal identities of Australian citizens, including through large-scale breaches of business customer data. Personal data, including identity information, is bought and sold on the dark web for a high price.

Identity theft can have devastating consequences for individuals. Recent high-profile cyber incidents have demonstrated the enduring harms experienced by Australians if their identities are stolen. Victims of identity theft may spend days or weeks trying to reclaim their stolen identities, facing significant financial loss. Currently, victims need to navigate a complex web of services and are often left to shoulder the emotional and financial burdens alone.

Diverse communities can be more vulnerable to cyber incidents and face additional barriers in seeking assistance. Culturally and linguistically diverse groups may face language barriers when seeking support. People who are hard of hearing may find it challenging to access support services if capacity constraints restrict in-person support. Other groups – including First Nations communities and seniors – face significant challenges if their identities are lost.

Beyond the personal toll on victims, identity theft has a substantial collective impact on society at large. The most recent survey in 2019 indicated that identity theft has cost Australia more than $3.1 billion[6] and has affected 20 per cent of Australians.[7] If identities can be easily stolen or defrauded, our communities may lose trust in our public institutions. Essential services that rely on digital identity verification – such as our financial and banking systems – could be at risk of severe disruption.

6. Australian Institute of Criminology (AIC) (2021). Identity crime and misuse in Australia: Results of the 2021 online survey.
7. AIC (2023). Cybercrime in Australia 2023.

How the Government will take action

The Australian Government aims to secure our identities from cyber attacks and provide better support to victims of identity crime.

Under this initiative, the Government will:

1. Expand the Digital ID program to help keep Australians' identities safe

The Government is continuing to develop the **Digital ID program** and the **National Strategy for Identity Resilience** to reduce the need for people to share sensitive personal information with government and businesses to access services online. This will mean fewer records of individuals' ID data and documents held by commercial and government organisations – reducing the risks and impact of identity theft and fraud. Cyber security of the Australian Government's Digital ID System is central to its design and the expanded program will continue to adopt best-practice cyber security standards such as ISO/IEC standards, the Australian Government's Protective Security Policy Framework, and the Australian Cyber Security Centre's Essential Eight to mitigate cyber security incidents. This is supplemented by additional protective security requirements specific to Digital ID for accredited providers participating in the Digital ID system.

2. Expand support services for victims of identity theft

The Government will **increase funding for victim support services** to help more individuals recover from identity theft to better protect themselves and other Australians. This will build on existing services provided by government and not-for-profit organisations and will be closely integrated with support services through cyber.gov.au.

This funding will enable case management services to allow individual victims of identity crime to obtain specialised support – including guidance on how to recover their identity, advice on how to mitigate damage and replace identity credentials, and education on warning signs that their identities continue to be misused.

Shield 2

Safe technology

Australians can trust that their digital products and services are safe, secure and fit for purpose.

What success looks like

Cyber security is a public good. By 2030, all Australians should feel protected by a secure and resilient digital economy. They should feel confident that cyber security will be enforced by those most capable of managing it across each layer of the technology supply chain.

Consumers and businesses will benefit from widespread adoption of cyber security standards across our technology and software markets. Our digital products will be secure by design and default. When purchasing digital devices or software, consumers should have peace of mind knowing that their technology is protected from cyber attacks and does not have embedded vulnerabilities that will put them or their families at risk.

In consultation, industry has called for a harmonised approach to cyber security standards for digital products. Our technology security standards will be designed to be consistent with international best-practice. Australia will work closely with industry and our international partners to design and align common security standards.

In addition to protecting our software and hardware, we also need to secure our data. Our most valuable datasets require adequate protections that keep pace with the current cyber landscape, without imposing unduly burdensome requirements on industry. This includes streamlined data retention requirements that are appropriate and proportionate.

We must also prepare for new and emerging technologies. The Government will continue to proactively support the development of emerging and critical technologies that have security at their core and safety in their design. By 2030, Australians should be able to safely embrace the opportunities presented by critical and emerging technologies – including quantum, AI, and advanced communications systems such as 6G.

How we'll get there

To achieve our 2030 vision, the Australian Government will:

- ensure Australians can trust their digital products and software;
- protect our most valuable datasets; and
- promote the safe use of emerging technology.

8 Ensure Australians can trust their digital products and software

The problem we face

Products and services without built-in security can present vulnerabilities that malicious actors can easily exploit, potentially undermining public trust in technology. Many digital products do not have security standards built in by design, or turned on by default. As a result, consumers and businesses can be offered less secure products and services, with insufficient expertise to manage the risk.

These market failures are particularly prevalent in the global 'Internet of Things' (IoT) or smart devices market, with the average Australian home set to have 33 connected devices by 2025.[8]

As the smart device market expands to include products like autonomous vehicles and distributed energy devices, these vulnerabilities could create systemic risks for society and the economy – and potentially facilitate cyber-enabled foreign interference.

8. Hughes, C, Average number of internet-connected devices per household in Australia in 2020 and 2021 with a forecast for 2025, Statista, Hamburg, 2023, accessed 14 November 2023.

How the Government will take action

The Australian Government will pursue a balance of voluntary and mandatory actions to enhance the security of our technology. These actions will provide end-users with confidence that their digital products are safe to use, without hindering industry innovation.

Under this initiative, the Government will:

1. Adopt international security standards for digital technologies

The Government will work with industry to encourage the adoption of international standards for secure-by-design in digital technologies such as IoT devices. In the short term, we will collaborate with industry experts to co-design options to legislate a **mandatory cyber security standard for IoT devices**. The standard could be aligned to international standards to ensure consistency between jurisdictions and minimise the regulatory burden on Australian businesses, while meeting our national security objectives.

To help consumers make informed choices about the security of devices on the market, the Government will also develop a **voluntary labelling scheme for consumer-grade smart devices**. These reforms will align Australia with international markets, including the United States, Singapore and the United Kingdom.

2. Embed cyber security into software development practices

The Government will work with industry and international partners to shape the development and adoption of international software security standards, including secure-by-design and secure-by-default practices. As a first step, we will work with industry and our international partners to co-design a **voluntary code of practice for app stores and app developers**. This code will clearly communicate expectations of cyber security in software development.

App stores are one of the best channels for intervention, as they are the single biggest marketplace to access consumer software. App stores also play a critical role in influencing software development practices by setting standards to screen products sold on their stores. The Government will work with industry to develop clear guidance on actions that app stores and developers can take to protect consumers and businesses from cyber attacks.

On the international stage, we will work with Quad partners to **harmonise software standards for government procurement**. Together with India, Japan and the United States, we are mapping our shared software standards and identifying opportunities to shift to common security standards. Aligning our standards will streamline procurement processes for industry, and our collective purchasing power will help set strong IT security standards across global markets.

3. Manage the national security risks of digital technology

The Government will develop a **framework for assessing the national security risks** presented by vendor products and services operating within and entering the Australian economy. Using this framework, the Government will help industry manage supply chain risks and make informed procurement decisions about the security of products and services. We will also consult industry on further options to limit the availability of non-secure products in the domestic market.

9 Protect our most valuable datasets

The problem we face

Data is an important source of growth for the Australian economy, helping organisations conduct transactions, make better decisions and improve their products and services. Businesses and global markets rely on the secure and free flow of data. Effective use of data helps Australian citizens get access to goods and services that are tailored to their needs.

In the wrong hands, data can allow malicious actors to do us harm. It can be held for ransom and used as a tool for coercion. Mishandling of sensitive and critical datasets can cause grave damage to Australia's national interests. Technological advancements have enabled malicious actors to develop vast data profiles on businesses, individuals and officials for intelligence-gathering and commercial purposes.

The *Privacy Act 1988* (the Privacy Act) covers the security of personal information held by entities with an annual turnover of more than $3 million. Recent reforms to the SOCI Act and the introduction of the Hosting Certification Framework for the Australian Government were vital steps in securing Australia's sensitive government and business data holdings. However, there is limited guidance for commercial, sensitive or critical datasets that fall outside the scope of these existing regulations.

There is also no common methodology by which the private sector can assess and communicate the value of data in a standardised way. Many businesses have voiced concerns that they are required to store substantial data records for excessive periods of time, which can often be high-value targets for malicious cyber actors. Some organisations take proactive steps to protect their data holdings, but this is often done in isolation, leading to inconsistent application of security controls and creating practical barriers to data sharing.

How the Government will take action

While the Australian Government has frameworks in place to protect personal information, we must continue to ensure that our data settings are fit for purpose as data increasingly becomes a resource to be collected, transferred and traded.

Under this initiative, the Government will:

1. Protect our datasets of national significance

The Government will **identify Australia's most sensitive and critical datasets** across the economy – particularly those that are not appropriately protected under existing regulations, yet are crucial to our national interests. This will allow us to assess whether existing data protections, including storage and governance settings, are proportionate and effective. Where gaps are identified that render these datasets vulnerable, the Government will explore options to better safeguard sensitive data across the economy.

2. Support data governance and security uplift across the economy

The Government will **review Commonwealth legislative data retention requirements**, with a focus on non-personal data, to determine whether existing provisions are appropriately balanced. Complementing our response to the Privacy Act Review, which will examine laws that require retention of personal information, the review will consider any unnecessary burden and vulnerabilities that arise from entities holding significant volumes of data for longer than necessary. Following the outcomes of this review, the Government will explore options to minimise and simplify data retention requirements.

The Government will **review the data brokerage ecosystem** to assess whether further action is required to address risks associated with the transfer of data to malicious actors via data markets. This review will complement the proposed reforms to the Privacy Act.

The Government will also **develop a voluntary data classification model**, offering guidance to help industry identify, assess and communicate the relative value of their data holdings in a consistent and unified way. This will enable businesses to segment information and implement proportionate operational controls, reducing enterprise risk.

10 Promote the safe use of emerging technology

The problem we face

Emerging technologies are delivering significant benefits across the economy and our society. As technological change accelerates, innovations are near impossible to predict, especially in the long term. Extraordinarily rapid growth in the functionality and scale of digital tools – including expansion in the capabilities of large language models like ChatGPT and text-to-image models like Stable Diffusion – make it difficult to plan for the future. Next-generation connectivity, such as autonomous vehicles or smart cities, will establish a new era of digital infrastructure. Advanced robotics systems will increase the pace of automation, boosting productivity in multiple sectors – including healthcare, manufacturing and agriculture. Building our capabilities in these technologies is important to ensure we can keep pace with change and leverage new opportunities as they emerge.

With increased reliance on critical and emerging technology comes the potential for an increased attack surface, expanding scope for malicious actors to attack our digital systems. We are already seeing significant cyber threats posed by these technologies, such as phishing attacks created by generative AI. As these develop, it will become increasingly difficult for the average person to distinguish legitimate communication from malicious attacks and fraud.

These technologies are also subject to immense strategic competition, and while presenting a range of benefits, could pose significant risks to our national interest. They will transform economic competitiveness, national and international security, as well as democratic governance and social cohesion. Australia must be ready, and ensure that our digital ecosystem is prepared for rapid transformation. Through continuous horizon scanning, and ongoing analysis of emerging technologies, we need to manage the risks and opportunities posed by these technologies.

How the Government will take action

The Australian Government is committed to supporting responsible innovation and advancements in emerging technologies throughout their full lifecycle, while retaining our strong stance on cyber security. The Strategy will support Government's efforts to address cyber and broader national security risks posed by critical and emerging technologies, including through enhanced industry, international and community engagement to ensure that these technologies are designed and developed in line with our interests.

Under this initiative, the Government will:

1. Support safe and responsible use of AI

Australia's world leading AI ethics principles were an important first step in developing and adopting trusted, secure and responsible AI. Following Australia's commitment to the Bletchley Declaration at the AI Safety Summit in November 2023, we will continue to work with other governments, civil society and the tech sector to ensure that AI is designed, developed, deployed, and used in a manner that is safe, secure, trustworthy and responsible. Our goal is to help ensure AI systems can be relied upon by Australians, while supporting innovation. This includes ensuring the right guardrails are in place, and supporting security by design, to ensure our citizens can trust the AI tools they use.

Building on our multimillion-dollar investment in Australia's AI capability, the Australian Government will continue to explore practical steps it can take to support the safe development and diffusion of AI technologies across the Australian economy, recognising the significant benefits they are already delivering and the significant future potential that they offer.

2. Prepare for a post-quantum world

The Government is already preparing for the possible disruptive impact of quantum computing. Advances in quantum computing could leave contemporary cryptography insecure, meaning that the technology we've become reliant on to protect our data will no longer keep our information safe. To prepare for these risks, we must anticipate future requirements of encrypted systems as we transition to post-quantum cryptography.

We will continue to monitor developments in quantum computing and **set standards for post-quantum cryptography**. This will include updating guidance in the Information Security Manual – ASD's publicly available cyber security framework that offers guidance for organisations on protecting their systems and data from cyber threats. Organisations will also be encouraged to prepare for the post-quantum future by conducting a review of their data holdings, and developing a plan to prioritise and protect sensitive and critical data. By keeping up to date with modern cryptographic algorithms, Australia will be best placed to ensure we can keep our information safe and secure.

Shield 3

World-class threat sharing and blocking

Australia has access to real-time threat data, and we can block threats at scale.

What success looks like

Australians should feel confident that the Government and industry are working together to identify and block cyber threats before they cause significant harm. Cyber threat intelligence sharing plays a crucial role in enhancing threat visibility across the economy, with collaboration between Government and industry helping to build a holistic threat picture. The Government draws on its access to expertise and information from classified sources to help businesses anticipate and respond to sophisticated cyber threats. Meanwhile, industry provides real-time data on emerging threats and vulnerabilities, helping the Government to enhance preparedness and response options.

New technologies and practices will inevitably shape the threat landscape and improve our capacity to share threat information at scale. By 2030, we will have a thriving whole-of-economy threat sharing and blocking network that will build on ASD's existing intelligence threat sharing platforms to enhance our ability to share cyber threat intelligence at machine speed across the nation. This network will include enhanced industry-to-industry information sharing, providing a multi-directional 'hub and spoke' model feeding data back into government threat intelligence systems and enabling information to be effectively distributed to industry. Real-time threat sharing will facilitate automated threat-blocking capabilities, enabling industry and the Government to block cyber threats before they reach end users.

How we'll get there

To achieve our 2030 vision, the Australian Government will:

- create a whole-of-economy threat intelligence network; and
- scale threat-blocking capabilities to stop cyber attacks.

Public-private partnerships in action

As recently announced by the Prime Minister and Microsoft on 24 October 2023, Microsoft will be investing $5 billion into the Australian technology and cyber security industry. A key element of this investment will be the co-led Microsoft-ASD Cyber Shield (MACS) which will further enhance existing efforts to increase national threat intelligence capabilities with a focus on detecting, analysing and defending Australia from sophisticated nation-state cyber threats. Other key elements of this investment include investing in digital infrastructure to support the growing demand for cloud computing services, investment to seize the opportunity AI offers, partnering with TAFE NSW to deliver a Microsoft Datacentre Academy to support this digital infrastructure and AI investment. These initiatives demonstrate how industry and government can work together to deliver a beneficial outcome for all Australians.

11 Create a whole-of-economy threat intelligence network

The problem we face

As cyber threats grow in scale and sophistication, a whole-of-economy threat picture is critical to build preparedness and mitigate risk. Existing initiatives, such as ASD's intelligence threat sharing platforms and the Cyber and Infrastructure Security Centre's Trusted Information Sharing Network, enable multi-directional government–industry and industry–industry threat intelligence sharing. However, industry has highlighted the need to improve national mechanisms to share strategic and tactical threat intelligence.

Industry-led threat intelligence sharing platforms continue to develop, including Intelligence Sharing and Analysis Centres (ISACs). However, more action is needed to promote cross-sectoral threat-intelligence sharing across industry. Some sectors have mature arrangements in place, such as the financial sector. Others, like the health sector, have less capability to share, receive or act on cyber threat information, leaving large parts of the economy lacking a comprehensive threat picture.

A holistic solution to cyber threat sharing requires enhanced government–industry and industry–industry engagement. But there is a risk of fragmentation if domestic ISACs and threat sharing platforms are not integrated with government threat sharing initiatives. We need to enable better collaboration between government and industry to improve the quantity, quality and speed of threat sharing.

How the Government will take action

The Australian Government will create a whole-of-economy threat sharing network through public–private partnerships that facilitate the rapid exchange of threat intelligence.

Under this initiative, the Government will:

1. Share strategic threat intelligence with industry

Industry has critical responsibilities to manage and mitigate cyber risk across the economy. To help industry respond to cyber threats, the Government will work with business leaders to facilitate genuine co-leadership on cyber security issues, enabled by improving industry's access to strategic threat intelligence. We will establish a **coalition of government and industry leaders** under the Executive Cyber Council. The Council will act as a key forum to build cross-sectoral trust and share strategic threat intelligence, in addition to driving public-private collaboration on other priority initiatives under the Strategy.

2. Expand tactical and operational threat intelligence sharing

The Government will invest in automated solutions to ensure we maintain visibility of threat activity across the economy. We will continue to **enhance ASD's existing threat sharing platforms**, co-designed with industry, to ensure that they can absorb expected future growth in the scale of cyber threat intelligence. This will amplify our ability to generate and share threat intelligence across the public and private sectors at machine speed, enabling organisations to move quickly to protect their networks when threats are identified.

The Government will also support industry-industry threat sharing by investing in a **Threat Sharing Acceleration Fund** to support the development of sector-specific ISAC in Australia. This fund will help build industry capabilities for intelligence collection and dissemination. This will be compatible with ASD's existing Cyber Threat Information Sharing platform and run knowledge-sharing programs to exchange best practice between industry members.

The Threat Sharing Acceleration Fund will start with an initial pilot for the health sector. Australians are rightly concerned about the cyber security of our health system – our hospitals and general practitioners hold some of the most sensitive data about Australians and their families. However, the health sector also has one of the lowest cyber maturities across industry. Through the Threat Sharing Acceleration Fund, the Government will seek to support the cyber security of Australia's health sector by helping health providers identify cyber threats and share best practice. This pilot will focus on building the capability of Australia's health system to identify threats and share intelligence between medical service providers.

By facilitating threat sharing between health providers, a Health ISAC will help industry address critical gaps in the cyber security of our health system. To ensure we develop a unified national threat picture, this ISAC will be integrated with existing government threat sharing platforms.

To promote uptake of threat sharing, the Government will **encourage and incentivise industry to participate in threat sharing** – with a particular focus on organisations most capable of collecting and sharing threat information at scale, such as critical infrastructure.

12 Scale threat blocking capabilities to stop cyber attacks

The problem we face

Threat intelligence sharing is essential to building a stronger threat picture, but it is only the first step. In order to effectively block threats at scale before they reach end users, threat intelligence must be put into action.

Australia's current approach to threat blocking is multifaceted, incorporating a mixture of technical capabilities, regulatory functions, and baseline mitigation strategies implemented by both government bodies and industry. Telecommunications and internet service providers (ISPs) have adopted a wide range of approaches to threat blocking. These entities need better access to high-confidence threat information to help them adopt comprehensive measures to block malicious cyber activity.

As threat actors become more sophisticated, it is essential for industry and government to share actionable, timely and contextualised threat intelligence to facilitate effective threat blocking capabilities.

How the Government will take action

The Australian Government is already building our national capability to block scams and harmful content through the launch of the National Anti-Scam Centre, as well as defining industry codes that specify responsibilities of the private sector in relation to scam activity. We have also made regulatory amendments to help telecommunications providers take proactive action to block threats. To further enhance our national threat blocking capabilities, the Australian Government will support and promote threat blocking across industry.

Under this initiative, the Government will:

1. Develop next-generation threat blocking capabilities

Building on existing work led by the National Anti-Scam Centre, the Government will support telecommunications and ISPs to block threats at scale. We have established a National Cyber Intel Partnership to develop cutting-edge threat blocking capabilities. Comprised of industry leaders and cyber experts from academia and civil society, the Steering Group is piloting the development of an automated, near-real-time threat blocking capability. These capabilities will build on, and integrate with, existing government and industry platforms. The Steering Group will inform the deployment of further threat blocking capabilities that can prevent identified threats from reaching end users.

As we build our threat intelligence sharing capabilities, we will develop more effective threat blocking technologies that work at machine speed and leverage machine learning algorithms to actively respond to the changing threat environment.

2. Expand the reach of threat blocking capabilities

Drawing on the work of the Steering Group, the Government will also seek to **encourage and incentivise threat blocking** across the economy by those most capable of doing so – including telecommunication providers and ISPs.

Shield 4

Protected critical infrastructure

Our critical infrastructure and essential government systems can withstand and bounce back from cyber attacks.

What success looks like

In 2030, every Australian should have peace of mind, knowing that essential services – such as our electricity grid, water supply and banking systems – are able to withstand and bounce back from hazards that might disrupt their functions. The array of critical infrastructure we rely on every day must be able to better prevent, respond, and be resilient to cyber attacks.

Owners and operators of critical infrastructure and designated Systems of National Significance need to have clear visibility of the risks they face – including cyber threats, personnel risks, physical hazards and natural disasters. Under the SOCI Act, they must put appropriate risk mitigation plans in place to protect against these threats. Through regulation and proactive collaboration, the Government will work with industry to provide a high level of assurance that owners and operators are complying with their security obligations.

The Australian Government will also lead by example. Government needs to hold itself to the same standard as it imposes on industry. As we increasingly adopt new and enhanced technology to support a range of government services, we will strive for a high level of cyber maturity, fostering public trust that we meet world-class cyber security standards. In doing so, we will work with state, territory and local governments to build a nationally consistent and robust culture of cyber resilience.

Figure 2: Australia's 11 designated critical infrastructure sectors

How we'll get there

To achieve our 2030 vision, the Australian Government will:

- clarify the scope of critical infrastructure regulation;
- strengthen cyber security obligations and compliance for critical infrastructure;
- uplift cyber security of the Commonwealth Government; and
- pressure-test our critical infrastructure to identify vulnerabilities.

13 Clarify the scope of critical infrastructure regulation

The problem we face

Australians must have confidence in the security and resilience of critical infrastructure sectors to deliver essential goods and services. Telecommunications and financial services should be resilient to major disruptions and external hazards. Energy, water and healthcare services, as well as food and grocery providers, should be available when we need them. Australians should not have to worry about suffering from the consequences of a cyber attack on unsecured critical infrastructure providers or their supply chains.

The SOCI Act provides a robust framework for defining and regulating the cyber security obligations for critical infrastructure. However, recent incidents have identified gaps in our cyber security regulation where it does not sufficiently cover specific sectors, entities or assets. In some cases, there are multiple regulatory frameworks that cover the same type of entity, creating unnecessary duplication and complexity. In other cases, obligations are unclear or some entities are not held to consistent cyber security standards.

How the Government will take action

The Australian Government will continue consultation with industry to ensure that our world leading critical infrastructure laws remain fit for purpose.

Under this initiative, the Government will:

1. Ensure we are protecting the right entities

The Government will work with industry to move the security regulation of the **telecommunications sector** from the Telecommunications Sector Security Reforms (TSSR) in the *Telecommunications Act 1997* to the SOCI Act. This will better align obligations for critical infrastructure entities that span multiple sectors, reduce regulatory duplication and complexity, and provide scalable obligations for the telecommunications sector.

The Government will also seek to clarify cyber security obligations for **managed service providers**, aligning closely with data protection initiatives established under Shield 2. Together, these initiatives will complement the protections and obligations for personal information established by the Privacy Act and action taken by the Government to strengthen individuals' trust in the management and storage of personal data.

The Government will explore options to incorporate cyber security regulation into 'all hazards' requirements for the **aviation and maritime sectors**. The Government will develop a reform agenda to strengthen Australia's aviation, maritime and offshore facility security settings, including positive obligations to proactively manage cyber-related risks under existing legislation. This will include stronger cyber security obligations on aviation, maritime and offshore facility regulated entities, including other critical infrastructure that enables international transport and shipping routes.

2. Ensure we are protecting the right assets

Government will also consult with industry to clarify the application of the SOCI Act to ensure critical infrastructure entities are adequately protecting their **data storage systems**. This consultation will focus on 'business-critical' data storage systems where vulnerabilities could impact the availability, integrity, reliability or confidentiality of critical infrastructure assets.

14 Strengthen cyber security obligations and compliance for critical infrastructure

The problem we face

Our critical infrastructure must be resilient to cyber threats in the face of heightened geopolitical risk, capable nation-state actors, and sophisticated cybercriminals. Cyber incidents affecting critical infrastructure entities may cause cascading impacts across the Australian economy due to our heavy reliance on their services.

Systems of National Significance are systems that would cause disproportionate damage to Australia's economy or national security if they were subjected to a cyber attack. To reduce the risk of major disruptions to our communities and businesses, these systems need to be able to withstand large-scale cyber attacks.

When cyber attacks are launched against our critical infrastructure and government systems, we must bounce back by responding and recovering quickly. However, responding to a cyber incident is not just about the technical event. Government and industry also need to work together to appropriately manage the ongoing consequences of a cyber attack. Following recent cyber incidents, critical infrastructure entities have called for better government support to help manage the ongoing impacts of an incident.

How the Government will take action

The Australian Government will continue to work closely with industry to defend our critical infrastructure and Systems of National Significance. We will protect these systems with multilayered defences to shield against the most sophisticated cyber attacks.

Under this initiative, the Government will:

1. Enhance cyber security obligations for Systems of National Significance

To protect our Systems of National Significance, the Government will expedite implementation of the **Systems of National Significance framework**. The framework will include Enhanced Cyber Security Obligations for these most vital systems, requiring them to have enhanced measures in place to ensure they bounce back quickly from a cyber attack.

The Government will also scale up ASD's Critical Infrastructure Uplift program, under which ASD's cyber experts partner with critical infrastructure providers to harden their networks.

2. Ensure critical infrastructure is compliant with cyber security obligations

The Government will ensure regulated entities are appropriately informed of their obligations under the SOCI Act – including the obligation to develop, maintain and comply with a critical infrastructure risk management program – by finalising a **compliance monitoring and evaluation framework**. As part of this framework, the Government will consult with industry on developing enhanced review and remedy powers, including the power to direct entities to uplift risk management plans if they are seriously deficient.

3. Help critical infrastructure manage the consequences of cyber incidents

The Government will consult with industry on how it can **help entities better manage the consequences of cyber incidents**. This includes the proposal to introduce a last resort all-hazards consequence management power to help industry deal with secondary consequences stemming from significant incidents, where no other Commonwealth, state or territory legislative levers are available to provide an effective response. Under this proposed power, Government would be able to authorise specific actions to manage consequences of a nationally significant incident, including cyber attacks or other hazards. Such powers reflect calls from critical infrastructure for enhanced government support when managing the ongoing impacts of an incident.

15 Uplift cyber security of the Commonwealth Government

The problem we face

The Australian Government needs to hold itself to the same standard it imposes on industry. Government is an owner and operator of critical infrastructure, and it also holds some of the most sensitive data about our people, economy and national security. As part of their core functions, Commonwealth, state, territory and local governments all provide essential services to our society. They form a critical part of our nation's digital infrastructure.

Government information and services can be high-value targets for malicious and state-sponsored threat actors. Cyber incidents can threaten the information held by the Government, public trust in our institutions, and the various digital functions that governments provide. For this reason, the Government has a vital role in setting best practice cyber security standards – a role recognised by nearly all stakeholders during consultation. Industry has clearly voiced an expectation that Government improves its own cyber security, in addition to imposing higher standards on other organisations.

Australia urgently needs a new approach to government cyber security. Enduring and low levels of cyber maturity across many Australian Government entities have revealed major gaps in our security posture. We have significant cyber skills shortages in the APS, and many government systems do not yet meet the ASD's Essential Eight strategies for mitigating cyber security incidents. To uplift our collective cyber security, the Government must itself adopt cyber best practices – including driving accountability for cyber security across its own departments and agencies.

How the Government will take action

Deliver a plan to uplift Commonwealth cyber security to position the Australian Government as a world-class trusted digital government.

Under this initiative, the Government will:

1. Strengthen the cyber maturity of government departments and agencies

The Cyber Coordinator will be enabled to lead whole-of-government cyber security uplift. As part of their role, the Coordinator will oversee the implementation and reporting of cyber maturity across Commonwealth departments and agencies. The Coordinator will also work collaboratively with state, territory and local governments to promote investment that will drive a meaningful shift in government cyber maturity.

To protect the Australian Government's data and digital estate, we will build on the best practice principles established within ASD's Essential Eight. We will also draw on internationally-recognised approaches to zero trust, aiming to **develop a whole-of-government zero trust culture**. We will implement defined controls across our networks that will be consolidated into the Australian Government Information Security Manual, and enabled through the Protective Security Policy Framework.

To provide ongoing accountability, we will develop an internal cyber security program and assurance function. We will scale up support to government entities uplifting their maturity against the Essential Eight. We will also **conduct regular reviews of the cyber maturity of Commonwealth entities** as part of the Investment Oversight Framework led by the Digital Transformation Agency. These reviews will inform further evolution of our security frameworks and help government entities meet changes in the evolving threat landscape.

2. Identify and protect critical systems across government

Government investments in cyber security must be focused on the systems that are most critical to our national interests, economic prosperity and social cohesion. To help prioritise our investments, we will designate **'Systems of Government Significance'** that need to be protected with higher security standards. We will map the Government's most important digital infrastructure, assessing the level of impact if these systems were disrupted.

3. Uplift the cyber skills of the Australian Public Service (APS)

The APS play a critical role in driving the cyber security posture across government. The Government will invest in **developing the cyber skills of the APS**, establishing a federated approach to growing and managing our in-house cyber capabilities.

16 Pressure-test our critical infrastructure to identify vulnerabilities

The problem we face

While this Strategy will better equip Australian citizens and businesses to protect themselves from cyber attacks, malicious actors will continue to identify and target vulnerabilities. To counter this, we need to stay ahead of the threat – we need to pressure-test our critical infrastructure to identify potential vulnerabilities before they are exploited.

All businesses should ensure that they are appropriately prepared to defend, respond to and recover from a cyber incident. However, the importance of critical infrastructure to maintain essential services necessitates a heightened level of readiness. In addition to identifying vulnerabilities in our networks, we also need to rehearse our incident response plans so that we are prepared for cyber incidents when they occur. By testing our national coordination mechanisms, it will be easier to get help and resume business continuity after an incident.

How will the Government take action

The Australian Government will build our national cyber readiness by proactively identifying and closing gaps in our cyber defences and incident response plans.

Under this initiative, the Government will:

1. Conduct national cyber security exercises across the economy

The Cyber Coordinator will lead a **National Cyber Exercise Program**, exercising the full spectrum of incidence response plans, consequence management and communications channels. Engaging closely across all sectors, the Government will exercise cyber incident scenarios to test established processes to support businesses and the economy in the event of an incident. These exercises will ensure that cyber crisis arrangements are understood, integrated and rehearsed.

This program will complement and build on the Enhanced Cyber Security Obligation to conduct exercises, applicable to Systems of National Significance under the SOCI Act.

2. Build playbooks for incident response

Running national exercises also presents a valuable opportunity to share cyber best practice across sectors. Operators and stakeholders will share strategies to identify opportunities for enhancement and further alignment across the nation in the event of an incident. Following these exercises, the Cyber Coordinator will develop **playbooks for incident response**. These playbooks will augment guidance to business leaders and lessons learned from the Cyber Incident Review Board under Shield 1.

Shield 5

Sovereign capabilities

Australia has a flourishing cyber industry, enabled by a diverse and professional cyber workforce.

What success looks like

By 2030, Australia will foster a thriving cyber security ecosystem that attracts, grows and retains talent, houses strong cyber security companies and capabilities, and nurtures innovative new technologies. Our nation will be recognised for pioneering work in cyber technology and applied sciences, with a large, skilled and diverse cyber workforce.

High-quality education and training opportunities will support defined pathways into the cyber security profession. Our cyber workforce will be professionalised, with clear standards to validate cyber skills and experience. By leveraging our existing commitments to landmark reforms across the immigration, education and training systems, we will assemble a world-class cyber workforce that welcomes people from a wide range of backgrounds. Our cyber workforce will be inclusive, with strong career opportunities for diverse cohorts – especially women, who are significantly underrepresented in the sector.

Australia will have a thriving and robust cyber security industry that supports national prosperity, generates high-wage jobs, and creates innovative solutions to current and future cyber security requirements. Cyber security firms will be supported by a robust market, with better opportunities to obtain government contracts and investment to stimulate growth.

Australia's strong academic and research institutions will continue to drive world leading cyber research and innovation. Through closer, focused collaboration between industry and government, we can tackle some of the toughest cyber security problems and invest in the secure development of emerging technologies like AI and quantum computing.

How we'll get there

To achieve our 2030 vision, the Australian Government will:

- grow and professionalise our national cyber workforce; and
- accelerate our local cyber industry, research and innovation.

17 Grow and professionalise our national cyber workforce

The problem we face

Industry suffers from ongoing shortages in the cyber security workforce, with a lack of representation of women and other diverse groups. Firms face challenges recruiting and retaining experienced world-class cyber talent – exacerbated by complex migration paths for foreign experts, and competition with higher pay rates abroad. AI and other emerging technologies are likely to transform cyber roles and reshape skill requirements as automated tools assume greater responsibility for core network protection functions.

Employers are facing a shortage of cyber professionals and a mismatch between job requirements and employee skills. A lack of sufficient job-ready experience is a key challenge for industry, with graduates and workforce entrants often requiring further on-the-job training to become proficient.

Improving the inclusivity and diversity of the cyber security workforce is imperative for the sector to reach its full potential. Beyond attracting more women and underrepresented cohorts into the cyber security sector, employers also have a role in fostering a workplace culture that is genuinely inclusive and embraces diversity. The cyber security sector needs to retain diverse talent to take advantage of a much wider spectrum of cyber skillsets, experiences and capabilities.

Industry has also identified inconsistencies across the Australian cyber security sector in meeting global cyber workforce standards. The absence of a national standard for cyber skills means employers lack assurance that the workforce is appropriately trained and that their qualifications are fit for purpose. To meet future cyber workforce needs, we need to transform our digital skills pipeline.

How the Government will take action

The Australian Government recognises that our cyber security workforce will constitute the foundation for sustained growth in the domestic cyber ecosystem. We will take immediate steps to foster a stronger, more diverse cyber security workforce – while providing businesses with greater confidence in the qualifications of cyber professionals.

Under this initiative, the Government will:

1. Grow and expand Australia's skills pipeline

The Australian Government has already commenced delivery of reforms to support and grow a more effective education and training system that will address Australia's digital and cyber security workforce needs. The newly established Jobs and Skills Australia and the Jobs and Skills Councils will work together to identify and meet future workforce needs, while also providing industry with a stronger voice, to deliver the best outcomes for learners and employers. This will include assessing workforce needs for cyber security skills.

The Government has taken steps to progress interventions at every stage of the skills pipeline. To encourage young people to pursue careers in the cyber workforce, learning cyber skills needs to start in primary and secondary school. The Government will continue to integrate cyber security teaching within Australian primary and secondary school education, in line with recent changes to the Australian Curriculum.

The Government is also making targeted investments at the graduate level by providing additional higher education Commonwealth Supported Places to support priority workforces, including in cyber, information technology and STEM (science, technology, engineering and mathematics) related fields.

Migration reforms will complement domestic skills pipeline initiatives to attract talent and make Australia a destination of choice for global cyber experts. The Government's **Migration Strategy** will establish a clear set of objectives for the migration system, bolstering our commitment to better coordination and integration of migration with the Australian labour market and training and education systems. A new global outreach capability and re-energised local outreach network will allow us to access critical talent pools and put Australia back in competition with other countries for the highly skilled migrants we need.

2. Improve the diversity of the cyber workforce

To create a diverse cyber workforce and tap into the potential of a broader market, the Government will work with industry to promote targeted support and return-to-work programs for women, underrepresented groups and diverse communities. The Government will also issue **cyber diversity guidance** to help employers attract and retain diverse cohorts into cyber security professions. This guidance will include specific recommendations on how to increase employment of women and First Nations people in cyber roles, acknowledging the major barriers they face to find and maintain jobs in the sector.

The Government will continue to consult with industry and work with the Executive Cyber Council to develop whole-of-economy initiatives to improve the diversity of the cyber workforce. The Government's response to the Pathway to Diversity in STEM Review will provide a further opportunity to consider concerted and systemic action to address this issue in the long term.

3. Professionalise the domestic cyber workforce

To support a thriving ecosystem, we will also work with industry to enhance efforts to **professionalise the cyber security workforce**. This will create clear pathways into cyber security roles, reduce barriers to entry and build greater consistency across the cyber workforce. A clear cyber skills framework will provide assurance to employers that the cyber workforce is appropriately skilled, and will give workers confidence that their qualifications and relevant experience are recognised and fit for purpose.

The Government's reforms to the vocational education and training (VET) system will provide training relevant to Australia's labour market and keep pace with emerging skills needs, including in critical areas like cyber security. This will be bolstered by a new five-year National Skills Agreement that will ensure a responsive VET sector provides the right training for critical and emerging industries. The Government will further invest in Australia's cyber security skills by offering ASD's cyber expertise to leading vocational training pathways and rolling out ASD's Essential Eight Assessment Course to TAFE's cyber consortium.

The Government has also asked the Australian Universities Accord to examine ways that tertiary qualifications can better align with skills needs – now and in the future. By connecting employers and tertiary institutions, we will promote a dynamic approach to shaping cyber qualifications to ensure graduates and apprentices are job ready and competitive in the workplace.

18 Accelerate our local cyber industry, research and innovation

The problem we face

Australia's cyber security industry supports our prosperity, generates new jobs and contributes over $2 billion to annual gross domestic product. However, the industry is hampered by challenges around workforce attraction and retention, translation of research and innovation into successful start-ups, and access to domestic and international markets.

Consultation with industry highlighted the Government's role as a potential customer to cyber security businesses and its ability to use its purchasing power to invest in new and innovative cyber products. Currently, a lack of home-grown capabilities deepens our dependence on offshore providers, undermining national sovereignty and stifling growth in this vital sector.

Sovereign capabilities need to be cultivated in key areas of our cyber ecosystem by investing in training pathways, commercial opportunities and research programs. We need to maintain ongoing investment in research and development of the cyber technologies that will underpin Australia's future digital economy.

How the Government will take action

The Australian Government will continue to identify and drive opportunities to grow the cyber security sector and invest in national cyber research programs.

Under this initiative, the Government will:

1. Invest in domestic cyber industry growth

We will promote the growth of innovative start-ups and small-to-medium enterprises by establishing a **Cyber Security Challenge program**, delivered through the existing Business Research and Innovation Initiative. This program will provide funding for cyber start-ups and small businesses to partner with government and develop innovative solutions to cyber security challenges facing Australia. This program will also support other key priorities outlined in this Strategy – such as developing cutting-edge technologies for threat sharing and blocking, or advancing post-quantum cryptographic techniques.

The Government's $15 billion National Reconstruction Fund (NRF) will also continue to support, diversify and transform Australia's key industries. The NRF will target projects and investments that help Australia capture high-value market opportunities to help businesses grow and succeed. It will provide finance to drive investments that develop capability in priority areas, including advanced information communication technologies, critical technologies including AI and quantum, and others relevant to cyber security.

The Government has also announced a $392.4 million Industry Growth program, through which innovative start-ups and small and medium enterprises will be able to receive support to commercialise ideas and grow their businesses. The program will provide advice and matched grant funding for projects in the NRF's priority areas, including those relating to cyber security. Companies' ability to expand and sell their products into priority international markets will also continue to be supported by Austrade's Landing Pads program.

Through the Buy Australian Plan, we will harness Government's purchasing power to support the cyber security sector in Australia. To further support the sector to flourish, we will work with industry to encourage the right kind of foreign investment in local cyber enterprises.

2. Maintain Australia's research capabilities

We will continue to support growth of the cyber security sector through measures reflecting our commitment to related research and development – including through Cooperative Research Centres and the Australian Research Council's Centres of Excellence and National Competitive Grants Program. Through the revitalisation of Australia's National Science and Research Priorities, the Government will explore options for further research efforts to drive innovation in cyber security and adjacent technologies.

Shield 6

Resilient region and global leadership

Australia's region is more cyber resilient, and is prospering from the digital economy. We continue to uphold international laws and norms and shape global rules and standards in line with our shared interests.

What success looks like

By 2030, Australia envisages a region better able to manage, mitigate and recover from the impacts of cyber incidents. Australia will continue to cooperate and build coalitions with international partners, industry and civil society to shape and advocate for rules, norms and standards that are consistent with our shared interests and values.

Australia will be the partner of choice for cyber security, with the trust and expertise required to manage increasing threats to the region; our regional efforts will deliver sustainable and shared cyber resilience. With our assistance, partners will have developed and retained the skills and capacity to be more cyber resilient. Though threats proliferate, few attacks will inflict significant damage, because protections are strong and recovery is swift. Increased resilience and strategic stability will ensure an open, stable and prosperous region, where citizens and businesses benefit from access to the global digital economy.

International standards for critical technologies will reflect Australia's interests and expertise. Global technology markets will be transparent and competitive, with a diversity of suppliers of products and services that are secure and safe by design. Australian citizens and businesses will reap the economic and security benefits of high-quality standards and digital trade rules.

A stable cyberspace will be supported by the agreed framework for responsible state behaviour. There will be clear consequences when states contravene their obligations and commitments. The internet will be open, free, secure and interoperable – with responsible and accountable multi-stakeholder management and governance.

How we'll get there

To achieve our 2030 vision, the Australian Government will:

- support a cyber resilient region as the partner of choice; and
- shape, uphold and defend international cyber rules, norms and standards.

19 Support a cyber resilient region as the partner of choice

The problem we face

Building cyber resilience is a shared global challenge. Countries in the region are experiencing the same scale and sophistication of cyber threats as we are, but many of our regional partners are trying to face this challenge from a lower base of security. As our region's reliance on the digital economy and connectivity grows, so does the need to strengthen regional capability and cyber resilience. Australia and international partners can better coordinate and enhance efforts to support our neighbours.

Geostrategic competition is playing out in the Indo-Pacific on multiple levels. Australia's security and prosperity are linked to our region and the implications of unchecked coercion and competition in our region are serious. Australia must maintain an active role to ensure strategic stability and prevent states with different values and strategic objectives from shaping the region according to their interests, at our collective expense.

How the Government will take action

The Australian Government will support cyber uplift among our neighbours. Australia will enhance cyber cooperation through existing forums, frameworks and initiatives. This includes bilateral, minilateral, multilateral and multistakeholder partnerships – such as the Quad and the Counter Ransomware Initiative. Australia will also build new partnerships and consider new mechanisms to coordinate and align collective efforts to lift cyber resilience, including with the Partners in the Blue Pacific. We will be guided through engagement with our Pacific and Southeast Asian partners, including as a member of the Pacific Islands Forum and through engagement with the Association of Southeast Asian Nations (ASEAN), to determine country-specific needs and regional priorities.

Under this initiative, the Government will:

1. Strengthen collective cyber resilience with neighbours in the Pacific and Southeast Asia

Australia will continue to work with our neighbours in the Pacific and Southeast Asia to build a more cyber resilient region. Our cooperation and assistance will continue to be coordinated by Australia's Ambassador for Cyber Affairs and Critical Technology.

We will refocus Australia's **cyber cooperation and capacity building efforts** to be more targeted, impactful and sustainable and to enable our neighbours to better prevent cyber incidents and recover quickly when they occur. Recognising that people engage with cyber security issues in different ways, our efforts will continue to consider gender equality, disability and social inclusion. This includes continuing support for the United Nations Women, Peace and Security agenda, as well as Australia's National Action Plan on Women, Peace and Security 2021–2031.

When severe cyber incidents occur in our region, Australia will be better positioned to respond to requests for assistance. Australia will establish a **regional cyber crisis response team** in the Department of Foreign Affairs and Trade, drawing on expertise from government, industry, and the technical community. In response to partner government requests following a significant cyber incident in the region, the team will help contain the spread and impact of cyber incidents and restore critical services and infrastructure.

2. Harness private sector innovation and expertise in the region

Industry can help drive an uplift in cyber maturity and security throughout our region. The Australian Government will work with regional governments, the private sector, and technical community partners to **pilot options to use technology to protect the region at scale**. We will leverage industry solutions to protect more people, systems and data from cyber threats.

Stronger connectivity will help businesses in our region securely access new opportunities in the global economy. We will use existing programs, including the Australian Infrastructure Financing Facility for the Pacific and the Quad Partnership for Cable Connectivity and Resilience, to strengthen undersea cable systems in the Indo-Pacific. Investments in cable infrastructure will enable connectivity and build cyber resilience in the region, including Australia's $78 million investment in subsea cable connectivity in the Pacific.

The private sector also has an important role to play in building security into all products. In line with our work on Safe Technology in Shield 2, Australia will work with manufacturers and technology providers to ensure countries in the region can access more secure products and services, so that they do not have to compromise between digital development and security.

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

The problem we face

As states with different principles impose their values through standards-setting forums, Australia must do more with international partners to defend and strengthen the international standardisation system, advocating for our shared interests and amplifying regional voices. As we increasingly rely on digital goods and services, we need to ensure digital trade rules provide better economic opportunities for businesses and consumers.

Cyber attacks on our democratic institutions or critical infrastructure are unacceptable. Malicious cyber activity globally can play an escalatory role in and around conflicts, including resulting in cascading critical infrastructure effects or disrupting humanitarian operations. States must act to uphold the agreed framework of responsible state behaviour in cyberspace, calling states out when they act contrary to this framework.

Across cyberspace we are increasingly seeing countries with interests at odds with our own trying to rewrite the existing and agreed rules. The ecosystem of technologies on which the internet depends also faces an enduring existential threat. We must defend the governance of this ecosystem and its multi-stakeholder model, to protect and promote a peaceful, stable and interoperable cyberspace.

How the Government will take action

Greater international engagement and cooperation makes Australia more stable, confident and secure at home, and more influential in the world.

Under this initiative, the Government will:

1. Support international standards for transparent and secure development of technology

Australia will protect and strengthen the international standardisation system. We will **promote robust international standards** in the technology underpinning cyberspace, the internet and the digital economy, including emerging technologies. Australia will work with global partners to ensure technology markets are transparent and competitive, with a diversity of suppliers for products and services that are secure and safe by design.

We will also seek to align with international best practice and support the established and effective approach to the development of international standards: industry-led and arrived at by consensus. We will support multi-stakeholder participation in standard setting to include relevant expertise and deliver outcomes consistent with our values and economic interests.

2. Advocate for high-quality digital trade rules

Australian businesses, workers and consumers benefit from an open, reliable and interoperable environment for digital trade. This means an environment that reinforces the international rules-based trading system and promotes trust in the online environment. Rules that support digital trade cooperation can help bridge digital divides and promote inclusion – both across and within national borders. Australia will continue to **drive development and implementation of high-quality digital trade rules** that address digital protectionism while maintaining appropriate flexibility to protect broader public policy interests.

3. Defend an open, free, secure and interoperable internet in international forums

Australia will also strengthen coalitions in our region to **defend the existing model for the internet**. We will continue to defend the technical infrastructure essential to the availability and integrity of the internet and its institutions, and oppose efforts to bring the technical management and governance of the internet under government control. We will do this by promoting the multi-stakeholder model of internet governance and strengthening the capacity for all stakeholders – including industry, civil society, academia and the technical community – to engage in internet governance mechanisms.

4. Uphold international law and norms of responsible state behaviour in cyberspace

We will collaborate with our existing partners and build new partnerships to **uphold international law and the agreed framework for responsible state behaviour** that underwrites our stability, prosperity, independence and sovereignty in cyberspace.

All countries have agreed to a rules-based cyberspace, founded on existing international law and norms. International law, complemented by agreed voluntary norms of responsible state behaviour, confidence-building measures and capacity building, provides a robust framework for predictability and stability in cyberspace. When implemented and adhered this framework provides a toolkit to address threats posed by state-generated and state-sponsored malicious cyber activity.

Australia will leverage our role as an honest broker in United Nations discussions to clarify how international law applies in cyberspace and strengthen implementation of the framework for responsible state behaviour in cyberspace. Such efforts will include enhancing cooperation through regional forums, including as part of the Pacific Islands Forum and through engagement with the ASEAN Regional Forum.

5. Deploy all arms of statecraft to deter and respond to malicious actors

Australia will deploy all arms of statecraft to **deter and respond to malicious cyber actors**. We will work with our international partners to take action to impose costs on individuals and organisations that make cyberspace less safe and secure. This includes calling out instances where states act to undermine or breach international law and norms, and imposing sanctions on those who carry out or facilitate significant cyber incidents – when we have sufficient evidence and it is in our national interests to do so.

In all its actions, Australia will uphold existing international law and the agreed voluntary norms of responsible state behaviour in cyberspace.

Next steps: Implementation and evaluation

How we will ensure we are on track to deliver

Implementation is central to achieving our vision. The Australian Government has developed the *Cyber Security Strategy Action Plan* (the Action Plan), which translates the commitments and initiatives in this Strategy into immediate actions to deliver concrete outcomes.

To ensure we deliver our initiatives, the Australian Government will:

1. Allocate resources to strategy implementation and governance

We have committed dedicated resources across government departments and agencies to deliver the initiatives in this Strategy. This includes funding for the implementation of specific initiatives, co-investment with industry partners, stakeholder engagement programs, and the overall governance and oversight of the delivery of the Strategy.

2. Define clear accountabilities for delivery

The Government has allocated clear accountabilities for each initiative in the Strategy. Our Action Plan identifies the lead agencies accountable for the delivery of each action, and supporting agencies that will enable implementation. The Cyber Coordinator will be responsible for whole-of-government coordination of the delivery of the Strategy – including collaboration with state, territory and local governments.

3. Continue close consultation with industry and the community

The Strategy has been developed in close consultation with industry and civil society. To achieve our 2030 vision, the Government will continue to adopt a genuine and transparent co-leadership approach, engaging in co-design wherever possible and ensuring our actions balance robust regulation and appropriate incentives.

After the launch of the Strategy, the Government will start a targeted consultation process to co-design specific initiatives with industry. This will include proposed legislative reforms, and other initiatives that will affect businesses and their cyber security obligations. This consultation process will directly inform the design and implementation of these initiatives.

The Government will also establish an **Executive Cyber Council** with industry leaders to support this consultation approach. Convening twice a year, this new strategic partnership will enable broader collaboration on national cyber security priorities, including initiatives driven under this Strategy. Comprising executives from across industry, the Council will complement other cyber governance groups, including the Data and Digital Ministers' Meeting and the Critical Infrastructure Advisory Council, to uplift Australia's cyber ecosystem through strong leadership.

4. Conduct robust evaluation of our progress

Implementation of the Strategy will be supported by robust evaluation of all initiatives. This will include assessment of the impact of individual initiatives and the effectiveness of the overall strategy in achieving our 2030 vision. We will continue to assess the nature of the threat environment and the strength of our national cyber shields to defend Australian citizens and businesses. This evaluation will be informed by feedback from industry and community leaders, threat intelligence, and lessons learned from cyber incidents.

5. Adapt our plan in response to changes in the cyber landscape

We will adopt a flexible approach to delivering this Strategy that adapts to the changing geopolitical landscape, threat environment and trends in the technology market. The Government will explore opportunities for new initiatives over the medium and long term, to ensure we continue to make meaningful progress towards our vision. To ensure our actions remain focused and fit for purpose, we will release an updated Action Plan every two years.

Our determination to implement the vision outlined in this Strategy will ensure Australia is positioned for enduring success and prosperity, underpinned by a world-class cyber security industry, a cyber-aware citizenry, effective and targeted government regulation, better support to industry, and deeper cooperation with international partners. We will be more resilient to cyber attacks and primed to respond ably and rapidly when they occur, to maintain the security and prosperity of our community and economy. Together, we can achieve our vision of becoming a world leader in cyber security by 2030.

Appendix A: List of acronyms

artificial intelligence	AI
Australian Federal Police	AFP
Association of Southeast Asian Nations	ASEAN
Australian Signals Directorate	ASD
Internet of Things	IoT
Information Sharing and Analysis Centre	ISAC
Privacy Act 1988	Privacy Act
science, technology, engineering and mathematics	STEM
Security of Critical Infrastructure Act 2018	SOCI Act
Telecommunications Sector Security Reforms	TSSR
vocational education and training	VET