AUSTRALIA'S CYBER SECURITY STRATEGY 2020 AT A GLANCE

Vision

A more secure online world for Australians, their businesses and the essential services upon which we all depend.

Approach

This vision will be delivered through complementary actions by governments, businesses and the community.

Cyber threats continue to evolve rapidly

- Cyber security threats are increasing. Nation states and state-sponsored actors and criminals are exploiting Australians by accessing sensitive information and for financial gain.
- Criminals are using the dark web to buy and sell stolen identities, illicit commodities, and child exploitation material, as well as to commit other crimes.
- Encryption and anonymising technologies allow criminals, terrorists and others to hide their identities and activities from law enforcement agencies.
- Cyber criminals want to take advantage of the fact that Australians are more connected than ever before.

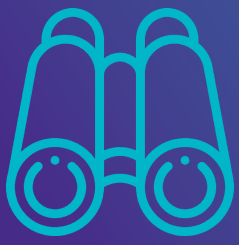
Strong foundations

This Strategy builds on the *2016 Cyber Security Strategy*, which invested $230 million to advance and protect Australia's interests online.

Highlights

This Strategy will invest $1.67 billion over 10 years to achieve our vision. This includes:

- Protecting and actively defending the critical infrastructure that all Australians rely on, including cyber security obligations for owners and operators.
- New ways to investigate and shut down cyber crime, including on the dark web.
- Stronger defences for Government networks and data.
- Greater collaboration to build Australia's cyber skills pipeline.
- Increased situational awareness and improved sharing of threat information.
- Stronger partnerships with industry through the Joint Cyber Security Centre program.
- Advice for small and medium enterprises to increase their cyber resilience.
- Clear guidance for businesses and consumers about securing Internet of Things devices.
- 24/7 cyber security advice hotline for SMEs and families.
- Improved community awareness of cyber security threats.



Overview

1. The Australian Government's vision is to create a more secure online world for Australians, their businesses and the essential services upon which we all depend.

2. The scale and sophistication of cyber threats continue to increase. Australians are increasingly reliant on the internet and the internet-connected devices we use daily. The digital economy is the future of Australia's economy. Our experience with the COVID-19 pandemic demonstrated this by highlighting how much Australians interact and work online, trusting the internet for healthcare, working from home, education, entertainment and online shopping. It is more important than ever to protect Australians online from those who would do us harm.

3. Australia's experience of COVID-19 has other lessons too. Just as we – governments, businesses, and the community – have relied on each other to fight the pandemic, cyber security relies on us all playing our part. Everyone – governments, businesses and the community – has a role to play in creating a more cyber secure Australia.

4. Cyber security allows families and businesses to prosper from the digital economy, just as pool fences provide peace of mind for households. Cyber security needs to be a fundamental and integrated part of everyday life, enabling Australians to reap the benefits of the internet safely and with confidence.

5. Through this Strategy, the Australian Government will build trust in the online world by supporting businesses' cyber resilience, including by sharing threat information, setting clear expectations of roles and strengthening partnerships.

6. The Australian Government will work with industry to protect our most critical systems from sophisticated threats. Law enforcement agencies will be given greater ability to protect Australians online, just as they do in the physical world, and will target criminal activity on the dark web. The Australian Government will confront illegal activity, including by using our offensive cyber capabilities against offshore criminals, consistent with international law. The Australian Government will continue to strengthen the defences of its networks, including against threats from sophisticated nation states and state-sponsored actors.

7 Businesses should produce secure products and services wherever possible as part of a strong and prosperous digital economy. A voluntary Code of Practice will set out the Australian Government's security expectations for the internet-connected consumer devices Australians use every day. The Australian Government will work with industry to consider and clarify the cyber security obligations of industry in the future, including through regulatory reforms.

8 Government and large businesses will assist small and medium enterprises (SMEs) to grow and increase their cyber security awareness and capability. The Australian Government will work with large businesses and service providers to provide SMEs with cyber security information and tools as part of 'bundles' of secure services (such as threat blocking, antivirus, and cyber security awareness training). Integrating cyber security products into other service offerings will help protect SMEs at scale and recognises that many businesses cannot employ dedicated cyber security staff. Governments will work hand in glove with critical infrastructure owners to identify and resolve immediate vulnerabilities. A Cyber Security National Workforce Growth Program will develop a skilled cyber workforce that can address emerging threats and new challenges, and maximise the benefits of the global economy's shift online.

9 Not all cyber security risks can be addressed by governments and industry – individuals should also take steps to protect themselves. The Australian Government will expand efforts to raise awareness of cyber security threats and empower the community to practise secure online behaviours. The Australian Government will offer a dedicated online cyber security training program, expanding our 24/7 cyber security advice hotline for SMEs and families, and increase funding for victim support services.

10 These measures will have the combined effect of making the internet more secure for all Australians. By ensuring the Australian Government can counter the most sophisticated threats and confront illegal behaviour, businesses and the community will be exposed to fewer risks and will suffer less harm. Australians will have greater confidence that essential systems are protected. Equipping small business owners and the community with the information and tools they need to protect themselves will encourage greater adoption of cyber secure products and cyber smart decision-making.

Strong foundations

The 2016 Cyber Security Strategy set out the Australian Government's plan to meet the dual challenges of the digital age – advancing and protecting Australia's interests online. The Australian Government backed the 2016 Strategy with a $230 million investment.

Feedback from businesses and the community showed that the 2016 Strategy strengthened Australia's cyber security foundations, stimulated private sector investment in the domestic cyber security industry, and positioned Australia as a regional cyber security leader. Key achievements include:

- Opening the Australian Cyber Security Centre (ACSC)
- Establishing Joint Cyber Security Centres (JCSCs) to engage state and territory governments and industry
- Increasing cyber skills and education investments
- Establishing the 24/7 Global Watch
- Appointing the Ambassador for Cyber Affairs
- Establishing AustCyber, the Australian Cyber Security Growth Network, and the Cyber Security Cooperative Research Centre.

This Strategy will build on initiatives that began in 2016, including the ACSC and JCSCs.

> *"Australia's landmark 2016 Cyber Security Strategy has been a catalyst for change, launching a series of government and private sector activities and responses to cyber security and cyber crime challenges."*
>
> **Palo Alto Networks**
> Public submission to the Cyber Security Strategy 2020

The threat environment

> *"The consequence of attacks are increasing in severity, as information systems become more central to business and society."*
>
> **Sapien Cyber**
> Public submission to the Cyber Security Strategy 2020

11 Cyber security is at the heart of the transition to a digital society. Cyber security is a key pillar in ensuring a trusted and secure digital economy, giving confidence to all participants and allowing businesses to prosper and thrive. The rapid and widespread uptake of digital technology by households and businesses following the COVID-19 pandemic underscores the importance of digital technology as an economic enabler. Millions of Australians are working from home, staying connected through apps and using essential digital services such as telehealth. Many bricks and mortar businesses are moving online for the first time – exemplified by revenue for the online shopping industry surging by 21.8% in March 2020 when viewed in year-on-year terms.[1]

12 To maximise the benefits of digital transformation, Australians must understand and address the threats that it can bring. Malicious cyber activity is one of the most significant threats impacting Australians. Between 1 July 2019 and 30 June 2020, the ACSC responded to 2,266 cyber security incidents at a rate of almost six per day. This does not include other incidents referred to the police and support organisations. The true volume of malicious activity in Australia is likely to be much higher. According to one expert analysis, cyber incidents targeting small, medium and large Australian businesses can cost the economy up to $29 billion per year, or 1.9% of Australia's gross domestic product (GDP).[2] Further, it is estimated that a four week interruption to digital infrastructures resulting from a significant cyber incident would cost the economy $30 billion (1.5% of Australia's Gross Domestic Product) and around 163,000 jobs.[3]

1 National Australia Bank (2020), NAB Online Retail Sales Index March 2020, available at https://business.nab.com.au/wp-content/uploads/2020/05/NAB-Online-Retail-Sales-Index-MAR20.pdf

2 Microsoft and Frost & Sullivan (2018), *Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World*

3 AustCyber (2020), Australia's Digital Trust Report 2020, available at https://www.austcyber.com/resource/digitaltrustreport2020

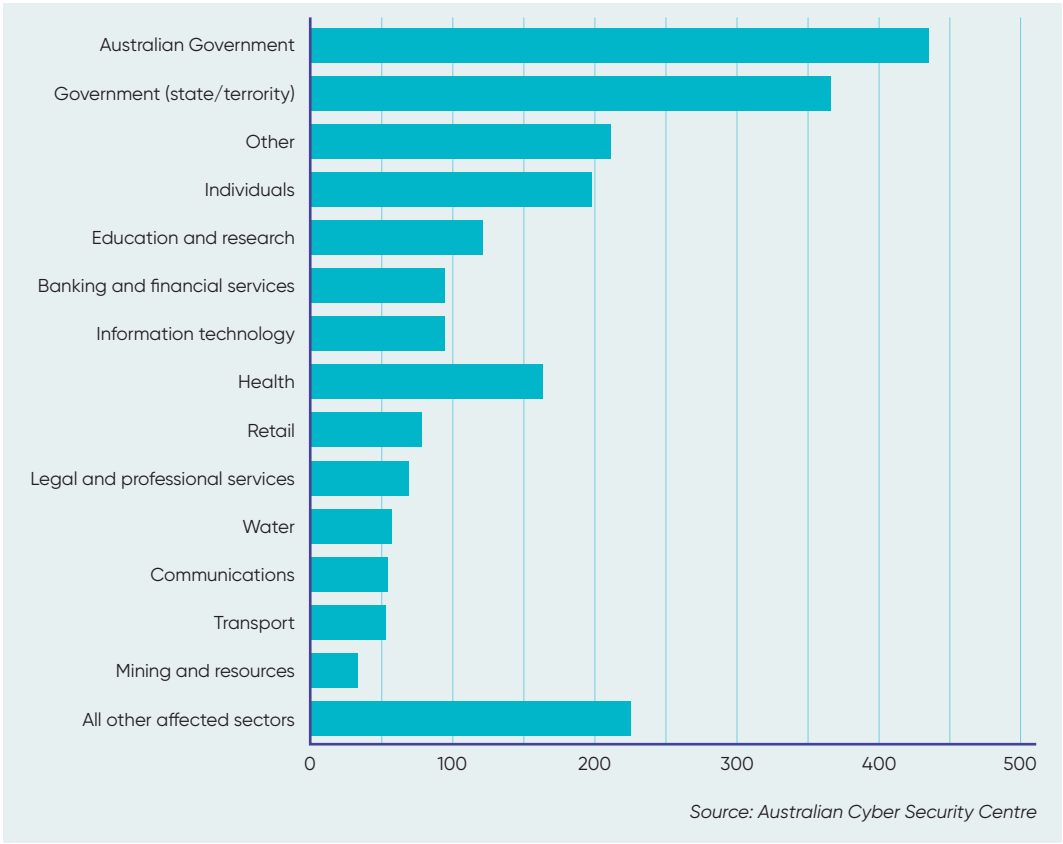
13 The COVID-19 pandemic highlighted the evolving nature of cyber threats. Opportunistic cyber criminals quickly adapted their methods to take advantage of more Australians working, studying and connecting online. Between 10 and 26 March 2020, the ACSC received over 45 pandemic themed cybercrime and cyber security incident reports, with the Australian Competition and Consumer Commission's (ACCC) Scamwatch receiving over 100 reports of COVID-19 themed scams. Campaigns were designed to distribute malicious software (malware) or harvest personal and financial information from unsuspecting Australians.

Cyber incident

A single event or a series of events that threatens the integrity, availability or confidentiality of digital information.

> *"Affordable and low-tech attacks such as ransomware, phishing and malware will continue to rise and a great emphasis from Government on supporting small to medium businesses and corporate Australia from cyber criminals is required."*
>
> **AUCloud**
> Public Submission to the Cyber Security Strategy 2020

Figure 1: Cyber security incidents, by sector (1 July 2019 to 30 June 2020)



Source: Australian Cyber Security Centre

Malicious cyber actors

14 Australians are being targeted by a range of different groups, varying in their intent and the sophistication of their tradecraft.

- **Nation states and state-sponsored actors** seek to compromise networks to obtain economic, policy, legal, defence and security information for their advantage. Nation states and state-sponsored actors may also seek to achieve disruptive or destructive effects against their targets during peacetime or in a conflict setting. These actors tend to be sophisticated, well-resourced and patient adversaries, whose actions could impact Australia's national security and economic prosperity.
- **Financially motivated criminals** exploit and access systems for financial gain, posing a substantial threat to the economic interests of Australia and the region. Of particular concern are transnational cyber crime syndicates, which develop, share, sell and use sophisticated cyber tools and techniques. Criminals are also using the dark web to buy and sell stolen identities, illicit commodities and child exploitation material, as well as to commit other crimes.

- **Issue-motivated groups and individuals** are primarily concerned with drawing attention to their causes. They are generally less capable and less sophisticated, but still able to cause significant disruption to industry and governments.
- **Terrorist groups and extremists** are effective at using the internet to communicate and generate attention, but generally employ very basic cyber techniques and capabilities such as distributed denial of service (DDoS) activities, hijacking social media accounts and defacing websites. These groups currently pose a relatively low cyber threat.

15 Highly sophisticated nation states and state-sponsored actors continue to target governments and critical infrastructure providers. Australian Government or state and territory government entities were targeted in 35.4% of the incidents the ACSC responded to in the year to 30 June 2020 (see Figure 1). Around 35% of incidents impacted critical infrastructure providers that deliver essential services including healthcare, education, banking, water, communications, transport and energy. A successful cyber attack against one of these services could have significant ramifications for the broader economy and Australian way of life. This is occurring overseas, as seen in the 2015 disruptions of power facilities in Ukraine, the 2017 Triton attacks on Saudi petrochemical facilities, and the NotPetya and WannaCry attacks in 2017 that impacted financial, transport and healthcare services across the globe.

16 In 2019, one in three Australian adults were impacted by cyber crime.[4] On average, the ACSC's ReportCyber tool receives a cyber crime report every 10 minutes. The barrier for entry into cyber criminal activity is very low. Underground online marketplaces offer cyber crime-as-a-service or access to high-end hacking tools that were once only available to nation states. Malicious actors with minimal technical expertise can purchase illicit tools and services to generate alternative income streams, launder the proceeds of traditional crimes or intrude into networks on behalf of more sophisticated adversaries.

4 NortonLifeLock (2020), 2019 Cyber Safety Insights Report Global Results, available at now.symassets.com/content/dam/norton/campaign/NortonReport/2020/2019_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf?

Malicious activity against Australian networks in 2020

On 19 June 2020, the Prime Minister announced that Australian organisations were being targeted by a sophisticated state-based cyber actor. This activity targeted Australian organisations across a range of sectors, including all levels of government; industry; political organisations; education, healthcare and essential service providers; and operators of other critical infrastructure.

The Australian Government knows it was a sophisticated state-based cyber actor because of the scale and nature of the targeting and the tradecraft used. The ACSC and the Department of Home Affairs have published a more detailed technical advisory with advice for Australian businesses and organisations to protect themselves. This advisory is available at cyber.gov.au.

Cyber criminals are taking advantage of the COVID-19 crisis to conduct widespread COVID-19-themed email and SMS phishing campaigns. These campaigns aim to distribute malware or harvest personal information from unsuspecting Australians.

To protect Australians, the Australian Signals Directorate (ASD) used its offensive cyber capabilities to disrupt foreign cyber criminals targeting Australian households and businesses. These offensive cyber operations struck back at the foreign criminals behind these COVID-19 themed phishing campaigns, successfully disabling their infrastructure and blocking their access to stolen information.

The ACSC also worked closely with Australia's major telecommunications providers and web-browser companies Google and Microsoft to disrupt these foreign criminals. These actions include flagging websites as malicious at the web-browser level and blocking them from phone users. This response showed how close partnerships between government and industry can protect Australians from malicious cyber activity.

Malicious cyber activity on the dark web

The dark web is the part of the internet that allows its users to remain anonymous. It is not easily accessible. The dark web facilitates illegal activity such as child sexual abuse, identity theft, drug and firearm trafficking and the planning of terror attacks.

The use of anonymising technologies has made it easier to commit serious crimes at volume and across jurisdictions. It allows criminals and other malicious actors to operate outside the visibility of law enforcement. If our law enforcement agencies are to remain effective in reducing cyber crime, their ability to tackle the volume and anonymity enabled by the dark web and encryption technologies must be enhanced. As part of this Strategy, the Australian Government will work to ensure law enforcement has the powers and capabilities to investigate and disrupt cyber crime, including on the dark web.

Consultation

17 On 6 September 2019 the Australian Government released a public discussion paper, '*A call for views*', to give every Australian a say in the development of this Strategy.

18 The Australian Government received 215 submissions from individuals and organisations, 156 of which are available at homeaffairs.gov.au/cybersecurity.

19 The Australian Government also met with more than 1,400 people from across the country in face-to-face consultations, including workshops, roundtables and bilateral meetings. There were also dedicated forums attended by representatives from large technology companies, academia, state and territory agencies, local governments and defence industry.

20 The following key themes were raised during the consultation process:

- The threat environment is worsening.
- Roles and responsibilities need clarification.
- Government and industry partnerships should be strengthened.
- Improved two-way information sharing is essential.
- Standards and regulation are necessary to get the basics right.
- Growth of cyber crime is outstripping our ability to respond.
- Many threats can be addressed at scale.
- Human behaviour is almost always part of the problem.
- Australia needs more trusted and skilled cyber security professionals.
- Small businesses are particularly vulnerable.
- Australia needs to be better prepared, especially for a national-scale incident.
- There are economic opportunities for Australia.

"ACCAN is concerned about the disproportionate impact that scams and other cybercrimes have on vulnerable consumers, such as those not confident in using the internet, older people and people who have less familiarity with the English language."

Australian Communications Consumer Action Network
Public submission to the Cyber Security Strategy 2020

"Just as there are vulnerable populations for public health concerns, we see this mirrored in vulnerable targets for cyber security attacks."

Accenture
Public submission to the Cyber Security Strategy 2020

"Government should be responsible for ensuring telecommunications operators, and operators of critical services take measures to safeguard networks and services."

Optus
Public submission to the Cyber Security Strategy 2020

Our Industry Advisory Panel

21 The Minister for Home Affairs (the Minister) also established an Industry Advisory Panel (the Panel) to provide strategic advice to support the development of *Australia's Cyber Security Strategy 2020*. The members of the Panel were:

- Mr Andrew Penn, CEO and Managing Director, Telstra (Chair)
- Ms Kirstjen Nielsen, former United States Secretary of Homeland Security
- Mr Robert Mansfield AO, Chair, Vocus Group
- Ms Robyn Denholm, Chair, Tesla
- Mr Chris Deeble AO CSC, Chief Executive, Northrop Grumman Australia
- Mr Darren Kane, Chief Security Officer, NBN Co.

22 The Panel met 13 times between November 2019 and July 2020, which included meetings with the Minister. The Panel structured its deliberations around 12 problem statements based on the key themes of feedback raised during the public consultation process. The Panel's final report provided recommendations covering seven key areas and is available at homeaffairs.gov.au/cybersecurity.

23 In line with the Panel's advice, this Strategy seeks to clearly set out the cyber security roles and responsibilities across government, businesses and the community as outlined in the next section.

24 Building on the success of the Panel, a standing Industry Advisory Committee will be established to ensure industry plays a continuing role in shaping the delivery of short and longer-term actions set out in this Strategy.

"Australia will prosper as a digital economy if we continue to invest in cyber defences. If we move to comprehensively protect ourselves from cyber-crime our businesses will remain competitive, our national infrastructure will be protected, the security of our institutions – including our democratic electoral processes, which have been the subject of malicious cyber-attack in other parts of the world – protected and the well-being of Australians improved. Acting quickly and decisively will also ensure the benefits outweigh the cost of remediation."

Andrew Penn
Chair of the Industry Advisory Panel and CEO of Telstra, August 2020

Our strategy

25 The Australian Government's Strategy is illustrated in Figure 2. The Australian Government's vision is for a more secure online world for Australians, their businesses and the essential services upon which we all depend.

Figure 2: Our Strategy Illustrated

Vision

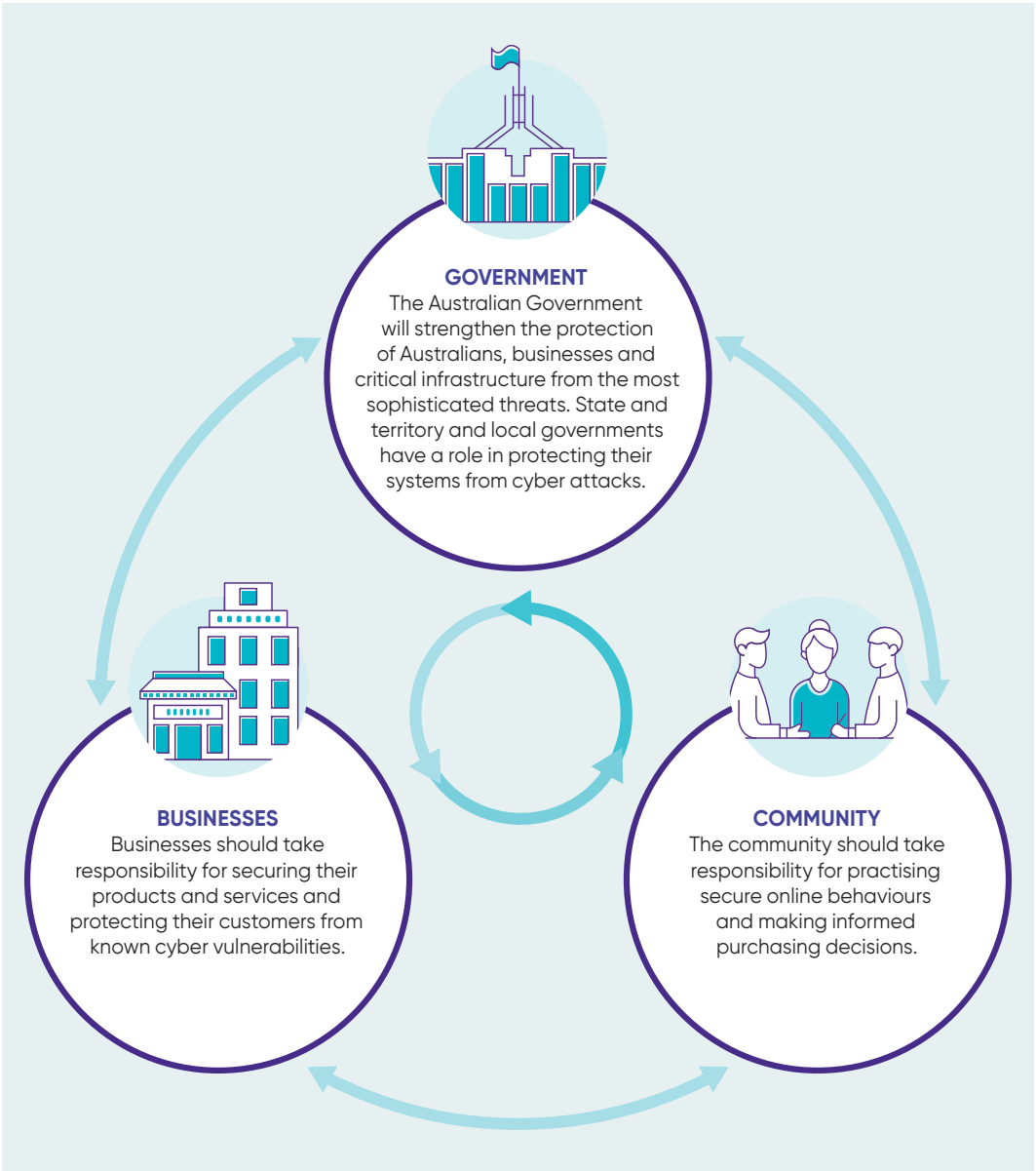
A more secure online world for Australians, their businesses and the essential services upon which we all depend.

Actions by governments	Actions by businesses	Actions by the community
Key themes: – Protect critical infrastructure, essential services and households – Combat cyber crime, including on the dark web – Protect Australian Government data and networks – Share threat information – Strengthen cyber security partnerships – Support business to meet cyber security standards – Enhance cyber security capabilities	**Key themes:** – Improve baseline security for critical infrastructure – Uplift the cyber security of SMEs – Provide secure products and services – Grow a skilled workforce – Take steps to block malicious activity at scale	**Key themes:** – Access and apply guidance and information on cyber security – Make informed purchasing decisions – Report cyber crime – Access help and support when needed

26 This vision will be delivered through action by governments, businesses and the community, as illustrated in Figure 3.

- The Australian Government will strengthen the protection of Australians, businesses and critical infrastructure from the most sophisticated threats. State and territory and local governments have a role in protecting their systems from cyber attacks.
- Businesses should take responsibility for securing their products and services and protecting their customers from known cyber vulnerabilities.
- The community should take responsibility for practising secure online behaviours and making informed purchasing decisions.

Figure 3: Roles and responsibilities in cyber security



27 This approach will enable Australia to make best use of its finite resources. The Australian Government will focus on critical threats and the most sophisticated actors, while ensuring a baseline level of cyber resilience across the economy. The Australian Government is best placed to deter and respond to sophisticated actors, including through defensive and offensive cyber capabilities. State and territory governments also have a role to play in ensuring their networks are not vulnerable to cyber intrusions.

28 Businesses should take responsibility for enhancing their cyber security, just as they are responsible for the safety and quality of their products. The Australian Government expects all businesses to play this role, and in the first instance will introduce legislation in relation to critical infrastructure and systems of national significance. Many of the initiatives in this Strategy aim to help businesses to take advantage of the digital economy by providing advice, practical tools and joint investment in a skilled workforce.

29 The community will always have a role to play in cyber security. Even with the best efforts of governments and businesses, Australians will need to know how to safeguard themselves against cyber security threats. This Strategy puts a greater focus on raising awareness of secure online behaviours, increasing access to victim support services and giving all Australians the information they need to make cyber secure purchasing decisions.

30 Every part of government, business and the community has a role to play in implementing this Strategy. Although this Strategy is an Australian Government initiative, the Australian Government recognises the essential role of state and territory governments, businesses, academia, international partners and the broader community in realising our vision: to create a more secure online world for Australians, their businesses and the essential services upon which we all depend. Successful implementation of this Strategy relies on individual and collaborative effort and actions by governments, businesses and the community.

Our response

Actions by governments

> *"Government has an important leadership role to play, which includes assisting organisations and the community to be fully cyber aware."*
>
> **Ai Group**
> Public submission to the Cyber Security Strategy 2020

31 The Australian Government is investing in its capabilities to respond to the growing cyber security threat. On 30 June 2020, the Australian Government announced the $1.35 billion Cyber Enhanced Situational Awareness and Response (CESAR) package. CESAR will ensure that ASD, as Australia's lead operational cyber security agency, can identify more cyber threats, disrupt more foreign cyber criminals, build more partnerships with industry and government, and protect more Australians. This section explains in detail the full suite of tools the Australian Government will use to address cyber security threats – from voluntary action and collaboration to legislation and classified capabilities.

Working in partnership with businesses

32 The Australian Government has a very important part to play in cyber security. It cannot protect all of cyberspace, but it will create an environment where everyone knows what role they play and what the 'rules of the road' are – including through legislation where necessary. This will allow businesses and the community to achieve greater national cyber security resilience so Australia can take advantage of the opportunities of an increasingly digital economy.

33 In addition to shaping policies to make Australia more secure online, the Australian Government has an important role to play in actively defending Australia from sophisticated malicious cyber actors. To achieve this, the Australian Government will target its cyber security efforts on the areas where it will make the most impact. In the shorter term, the initial focus is on setting expectations for critical infrastructure and systems of national significance (set out in further detail under 'Actions by businesses'). This will involve ensuring Australia has the right policies and capabilities in place to manage the highest consequence threats to Australia to protect the essential services on which all Australians depend for our way of life.

34 Although Australia has been lucky to avoid a catastrophic cyber security incident, we are vulnerable to the cyber attacks experienced elsewhere in the world. Supporting the continuity of essential services in the face of disruptive or sophisticated attacks is a fundamental obligation for government. The loss of an essential service like electricity, water or transport could have devastating impacts across Australia far beyond the targeted business. Although more can be done to raise the overall security posture of critical infrastructure (see 'Securing essential services' section), some nation states or state-sponsored actors are so sophisticated that an attack may be beyond the capability of a single network owner to handle alone, irrespective of its size, expertise and best efforts.

35 The Australian Government must be ready to act in the national interest when its unique capabilities are needed, especially in emergency situations. In consultation with critical infrastructure owners and operators, the Australian Government will develop new powers proportionate to the consequences of a sophisticated and catastrophic cyber attack, accompanied by appropriate safeguards and oversight mechanisms. These powers will ensure the Australian Government can actively defend networks and help the private sector recover in the event of a cyber attack. The nature of this assistance will depend on the circumstances, but could include expert advice, direct assistance or the use of classified tools. This will reduce the potential down-time of essential services and the impact of cyber attacks on Australians.

36 The Australian Government will also work with businesses to consider legislative changes that set a minimum cyber security baseline across the economy. This consultation will consider multiple reform options, including:

- the role of privacy, consumer and data protection laws
- duties for company directors and other business entities
- obligations on manufacturers of internet connected devices.

This consultation will examine ways to simplify and reduce the cost of meeting any future minimum baseline.

37 The Australian Government will strengthen its capacity to prevent or respond to malicious cyber activity, including in response to sophisticated actors. Through this Strategy, the Australian Government will invest $62.3 million in a classified national situational awareness capability to better enable government to understand and respond to cyber threats to critical infrastructure and other high priority networks. This will be complemented by increased incident reporting and near-real-time threat information from the most essential pieces of infrastructure as part of future regulatory requirements. To make use of all sources of threat information, the Australian Government will deliver an enhanced threat-sharing platform, enabling critical infrastructure operators to share intelligence about malicious cyber activity with government and other providers at machine speed, and block emerging threats as they occur. This Strategy will invest $118 million to expand ASD's data science capabilities. The Australian Government will invest $66.5 million to assist Australia's major critical infrastructure providers to assess vulnerabilities to enhance their cyber security posture. An additional $20.2 million will go to cutting-edge research laboratories so we can better understand threats to technologies that underpin Australia's critical infrastructure systems on which businesses and home users increasingly rely.

38 This requires strong partnerships between businesses and governments. To support the partnership, the Australian Government will increase its investment in the JCSCs in Sydney, Melbourne, Brisbane, Perth, and Adelaide, and expand the number of services available to our partners. Continuing and expanding the JCSCs was strongly supported during public consultation. Strengthened JCSCs will accommodate an increased number of cyber outreach officers, including from the Department of Home Affairs. These outreach officers will be a crucial link in developing strong partnerships and sharing actionable cyber security advice.

39 All JCSCs will include multi-classification facilities to accommodate a broader range of ACSC capabilities and classified engagement with law enforcement and trusted partners. The number of technical staff will also be increased, creating multi-disciplinary teams of experts who can provide additional operational and technical expertise across the nation. The work of the enhanced JCSCs will complement that of growing and vital private cyber security businesses.

40 Although the cyber security of the tertiary education sector is primarily the tertiary education sector's responsibility, the Australian Government is also investing $1.6 million to enhance the cyber security of Australian universities. This will fund a threat intelligence-sharing network, sector-wide threat modelling and a national cyber security forum that will meet three times a year. Strengthening the collective defences of universities against future threats will support our cyber skills agenda. The Australian Government welcomes the work that Australia's Academic Research Network (AARNet) is doing to share threat intelligence within the tertiary education sector.

41 The Australian Government will also work closely with businesses to prepare for cyber incidents by practising our incident response procedures. An expanded cyber security incident exercise program, led by the ACSC, will ensure that Australian businesses and governments have practised their incident responses ahead of time and are always strengthening their readiness and resilience. The Australian Government will work with state and territory governments on formally recognising businesses in governments' incident response playbook, known as the Cyber Incident Management Arrangements. This will ensure that all parts of Australia's society have clearly defined roles and responsibilities and know what to do in the case of a national cyber incident or emergency.

Holding cyber criminals to account

42 Tackling crime is just as important in the online world as it is in the physical world. Criminals from anywhere across the globe can use the internet to harm Australians with ease and at scale. To hold cyber criminals to account and prevent cyber crime, law enforcement agencies across Australia will need to work together. Building on the success of approaches to counter terrorism and child exploitation, this Strategy will encourage even greater cooperation across Australia and with international partners. The Australian Government will work with state and territory governments to prioritise our efforts and equip agencies with the capabilities to make a difference. The Australian Government will also bolster the Australian Federal Police's (AFP) ability to investigate and prosecute cyber criminals, investing $89.9 million. This investment will enable the AFP to establish target development teams with partners, build technical cyber capabilities and enhance operational capacity. The Australian Transaction Reports and Analysis Centre's financial intelligence expertise will be harnessed to target the profits of cyber criminals. Building on the establishment of a countering foreign cyber criminals capability in 2019, the Australian Government will also further expand the ACSC's ability to counter cyber crime actors offshore.

43 Encryption is an important way of protecting consumer and business data, but the increasing use of the dark web and encryption technologies that allow people to remain anonymous online is challenging law enforcement agencies' ability to protect our community. The dark web enables cyber criminals to broadcast child sexual exploitation and abuse, trade in stolen identities, traffic drugs and firearms, and plan terror attacks. These platforms make committing serious crimes at volume, and across borders, easier than ever before. The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* introduced in 2018 has helped Australia's law enforcement and security agencies, working with industry, tackle online criminal and terrorist threats. Through this Strategy, the Australian Government will ensure law enforcement agencies have appropriate legislative powers and technical capabilities to deter, disrupt and defeat the criminal exploitation of anonymising technology and the dark web.

Identifying threats

44 Australia's law enforcement agencies face a continuous challenge to identify new threats before these threats harm Australians, and to respond to technological developments. The Australian Signals Directorate will recruit 500 additional intelligence and cyber security personnel at a cost of $469.7 million over 10 years. The Australian Government will invest $385.4 million in enabling and enhancing intelligence capabilities. In addition to holding cyber criminals and malicious actors to account, these steps will ensure that Australia remains a world leader in developing new and innovative approaches that enable all Australians to securely adopt new technology and access the benefits of the digital economy.

Government systems

45 Governments also have a responsibility to lead by example. Shifting more government services online is making the lives of Australians easier. However, citizens need to have confidence that their data is safe, underscoring the need for government systems and data to be secure. This Strategy will drive long-term work by the Australian Government to strengthen the defences of Commonwealth public sector networks. The first priority is to centralise the management and operations of

the large number of networks run by Australian Government agencies, including considering secure hubs. Centralisation could reduce the number of targets available to hostile actors such as nation states or state-sponsored adversaries, and allow the Australian Government to focus its cyber security investment on a smaller number of more secure networks. A centralised model will be designed to promote innovation and agility while still achieving economies of scale.

46 The centralisation of cyber security systems across government will be complemented by the work of Australian Government agencies to strengthen their cyber security and implement the ACSC's Essential Eight mitigation strategies. This work will be informed and supported by the ACSC's ongoing technical cyber security advice and guidance. This approach to the uplift of government systems will be designed to reduce the risk of compromise, and help to prevent the most common techniques used by malicious cyber actors. Australian government agencies will also put a renewed focus on policies and procedures to manage cyber security risks. Standard cyber security clauses will be included in Australian Government IT contracts.

The connection between cyber crime and identity theft

Many cyber threats are enabled by malicious actors concealing their identities using fake or stolen identity information. Personal information stolen from innocent Australians is widely available in thriving dark web markets, where it is bought and sold on an industrial scale by criminals looking to commit fraud or facilitate other illegal activities. For example, criminals use stolen identities to withdraw money from bank accounts, take out loans, apply for credit cards, or claim government benefits in another person's name.

Trusted digital identities promote cyber security

47 To help protect Australians against identity crime, the Australian Government's Digital Identity program gives people the choice to use a trusted digital identity credential, such as a myGovID, to access online services from participating government and private sector organisations. This will make accessing online services easier and safer for Australians, while giving organisations greater confidence in who they are dealing with online.

48 By using trusted digital identity credentials to access multiple online services, people will not need to repeatedly re-verify their identities or maintain multiple passwords. This reduces the amount of personal information that needs to be shared with online service providers, helping to prevent identity theft and other forms of cyber crime.

49 Trusted digital identities need to be verified against government identity records such as passports, driver licences and birth certificates – documents Australians rely on every day to help prove their identities. The Australian Government will work with states and territories to update the National Identity Security Strategy to strengthen arrangements for issuing and managing these documents, maintain strong privacy safeguards, and further bolster our defences against identity and cyber crime.

International engagement

50 Finally, governments have a responsibility to uphold existing international law and norms of responsible state behaviour in cyberspace. Australia will continue to encourage the international community to act responsibly online, including by complying with existing international law, domestic law and norms of responsible state behaviour. The Australian Government will ensure that Australia is not seen as a soft target and will continue to publicly call out countries when it is in our interests to do so. The Australian Government will match its public statements with action through a range of targeted and decisive responses against unacceptable intrusions or activity in line with Australia's statement of principles on cyber deterrence:

We work to actively prevent cyber attacks, minimise damage, and respond to malicious cyber activity directed against our national interests. We deny and deter, while balancing the risk of escalation. Our actions are lawful and aligned with the values we seek to uphold, and will therefore be proportionate, always contextual, and collaborative. We can choose not to respond.

51 The Australian Government's actions will strengthen the nation's cyber security. Stronger obligations and partnerships will give us the best chance of disrupting or minimising sophisticated attacks. Bolstered law enforcement and intelligence capabilities will create a stronger deterrence against cyber criminals. Government systems on which all Australians rely will be hardened. The actions required of businesses will build on these initiatives.

Australia's Cyber and Critical Technology International Engagement Strategy

The Australian Government defines critical technology as current and emerging technologies that have the capacity to significantly enhance or pose a risk to our national interest (prosperity, social cohesion or national security). Critical technology and cyberspace are becoming increasingly important aspects of international relations. They are intrinsically linked to our national prosperity and security; the protection and promotion of human rights and democracy; international stability; global economic prosperity; and sustainable development.

The Australian Government is developing a Cyber and Critical Technology International Engagement Strategy. Building on the *2017 International Cyber Engagement Strategy*, the next Cyber and Critical Technology International Engagement Strategy will provide a framework to guide Australia's international engagement, to ensure cyberspace and critical technology support our goal of a safe, secure and prosperous Australia, Indo-Pacific and world. This includes partnerships to support the achievement of our cyber security goals by building international capacity and resilience to cyber security threats, cyber crime, online harms and disinformation.

The Australian Government will place an increased focus on engaging internationally on the security of critical technologies. The nature of global supply chains means that Australia needs to take joint action with likeminded countries to ensure these critical technologies are not manipulated for malicious purposes.

Working with international partners

The security and resilience of our allies, regional partners and the broader international community is vital to ensuring Australia's own national security and prosperity.

Australia is committed to supporting and sustaining international mechanisms that promote stability, and to working with partners on a voluntary basis to deter and respond to unacceptable behaviour in cyberspace.

Australia contributes to forums such as the International Organization for Standardization and the International Telecommunication Union which develop international standards that contribute to a more secure cyberspace for all countries.

Awareness raising and capacity building helps ensure the peaceful use of technology, and will ultimately enhance our collective cyber resilience and thus deliver direct benefits for Australia. Some countries may require assistance in their efforts to:

- improve the security of critical information and communications technology (ICT) infrastructure
- develop technical skills and appropriate legislation, regulatory frameworks and strategies to fulfil their responsibilities
- bridge the divide between the security of ICT and its use.

Building the capacity of our neighbours

The Australian Government has already committed $60 million to support cyber capacity building in the Indo-Pacific region to champion an open, free and secure cyberspace. This includes a seven-year, $34 million Cyber Cooperation Program, working with government, industry, civil society and academia to enhance cyber resilience across the full spectrum of cyber affairs. The Cyber Cooperation Program is now also working to mitigate the impact of malicious cyber activity during COVID-19.

Australia has also committed to a four-year, $14 million Australia-Papua New Guinea (PNG) Cyber Security Cooperation initiative to enhance PNG's cyber security frameworks and technical capability, and a four-year $12.7 million Australia-India Cyber and Critical Technology Partnership.

Actions by businesses

> *"In our connected economy, an attack on one organisation can have impacts across customers and supply chains."*
>
> **Commonwealth Bank of Australia**
> Public submission to the Cyber Security Strategy 2020

52 Cyber security is important to all businesses. It provides access to the digital economy and protects hard-earned profits, valuable intellectual property and sensitive customer data. Some businesses take cyber security more seriously than others. Given the private sector owns most of Australia's data and networks, Australia will not be secure until all businesses take steps to protect themselves, their supply chains and their customers.

Securing essential services

53 The best way to protect Australians at scale is to secure our critical infrastructure. Through this Strategy, the Australian Government will work with owners and operators to uplift their cyber security and to actively defend networks, using both defensive and offensive tools. This is consistent with feedback from consultation on this Strategy about working together to better defend critical infrastructure.

54 The Australian Government takes seriously the need to protect our critical infrastructure and has already taken action to do so. The Australian Government introduced reforms in 2018 to manage threats to the telecommunications sector and certain electricity, water, gas and port assets. However, the threat environment is worsening. In response to this, the Australian Government is developing an enhanced regulatory framework for critical infrastructure and systems of national significance.

55 The enhanced framework will uplift security and resilience in critical infrastructure sectors, combined with better identification and sharing of information about threats in order to make Australia's critical infrastructure – whether owned or operated by industry or government – more resilient and secure. This approach will prioritise acting ahead of an incident wherever possible.

56 One size does not fit all. The framework will balance objectives for cyber, physical, personnel and supply chain protections across all sectors, while recognising sector-specific differences. This is why the framework will be built around principles-based outcomes, underpinned by guidance and advice proportionate to the risks and circumstances in each sector. Due to the interconnected nature of critical infrastructure sectors, even mature sectors will benefit from these changes and they should see an uplift in their supply chain as well as the networks and systems that they depend on.

57 This framework will apply to owners and operators of relevant critical infrastructure regardless of ownership arrangements. This creates an even playing field for owners and operators and maintains Australia's existing open investment settings, ensuring businesses that take security seriously are not at a commercial disadvantage.

58 Australia's enhanced critical infrastructure security regulatory framework will clarify what infrastructure owners need to do to meet our minimum expectations of cyber security. It will include:

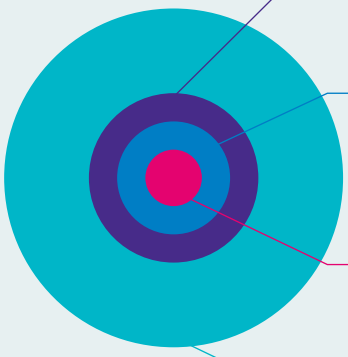
- an enforceable positive security obligation for designated critical infrastructure entities;
- enhanced cyber security obligations for those entities most important to the nation
- Australian Government assistance for businesses in response to the most significant cyber attacks to Australian systems
- voluntary measures to strengthen engagement with businesses in relation to risk, and support an entity's security uplift.

59 This enhanced regulatory framework will be delivered through amendments to the *Security of Critical Infrastructure Act 2018*.

Protecting critical infrastructure and systems of national significance

The *Telecommunications Sector Security Reforms and Security of Critical Infrastructure Act 2018* strengthen Australia's protection against threats to the telecommunications sector and certain electricity, water, gas and port assets.

The Australian Government will build on this foundation to include other critical sectors that Australians rely on for our way of life. As part of these reforms, the Australian Government will introduce obligations for the owners of these regulated critical infrastructure assets, including further cyber specific obligations to protect our most critical systems.



Critical Infrastructure Entities

Description: All entities within expanded *Security of Critical Infrastructure Act 2018* designated critical infrastructure sectors

Framework elements: Government Assistance (directions and direct action)

Regulated Critical Infrastructure Entities

Description: *Security of Critical Infrastructure Act 2018* designated critical infrastructure entities

Framework elements: Positive Security Obligation; Government Assistance (directions and direct action)

Systems of National Significance

Description: The subset of critical infrastructure entities of highest criticality

Framework elements: Enhanced Cyber Security Obligations; Positive Security Obligation; Government Assistance (directions and direct action)

Whole of economy

These reforms will also recognise that although entities have a responsibility to take steps to protect themselves and the services they deliver, the Australian Government has an obligation to act in the national interest when the threats or consequences are too high for individual entities to manage without its unique capabilities.

60 At the other end of the scale, SMEs are especially vulnerable to cyber security threats. Feedback from consultation shows SMEs often lack the resources or expertise to defend themselves and that there can be a large impact on regional communities when cyber criminals target SMEs. This Strategy includes an $8.3 million Cyber Security Connect and Protect Program, which will assist SMEs through tailored advice and assistance from trusted sources.

61 The Australian Government will also provide online training and a 24/7 helpdesk for SMEs that needs cyber security advice or assistance. Government and large businesses will assist small businesses to upgrade their cyber security and grow their cyber security awareness. The Australian Government will encourage large businesses and services providers to provide small businesses with cyber security information and tools as part of 'bundles' of secure services, such as threat-blocking, antivirus and cyber security awareness training. Integrating cyber security products into other service offerings will help protect SMEs at scale and recognises that many businesses cannot employ dedicated cyber security staff. All of these programs will continue to be brought together on cyber.gov.au, so that SMEs can quickly find the Australian Government assistance that best meets their needs.

Supporting SMEs

The Australian Government will prioritise support for SMEs through a number of key initiatives:

- A $12.3 million expansion to the ACSC's 24/7 cyber security hotline will enhance the provision of cyber security advice and technical assistance.
- The $8.3 million Cyber Security Connect and Protect Program will equip trusted organisations to raise the cyber security of SMEs in their local area.
- The placement of outreach officers in Joint Cyber Security Centres will support SMEs.
- Supporting the roll-out of threat-blocking technology will prevent known malicious cyber threats from reaching Australian consumers and businesses.
- The ACSC Small Business Cyber Security Guide provides tailored advice to protect against the most common cyber security incidents.
- ACSC-produced Step-by-Step and Quick Wins Guides provide practical instructions with visual aids outlining actions SMEs can take to protect themselves.
- The ACSC Stay Smart Online Program promotes best practice cyber security advice and encourages businesses to protect themselves online.
- Toolkits published on cyber.gov.au will help SMEs raise cyber security awareness among their staff members.
- A dedicated online cyber security training program hosted on cyber.gov.au will help upskill SMEs and their staff members.
- Law enforcement will have strengthened capabilities to identify and disrupt cyber criminals targeting Australian businesses.

"Today, cyberattacks from increasingly sophisticated actors threaten organisations across every sector, and whether a large ASX 100 company or a local bakery, organisations of all sizes need to take steps to limit the dangers posed by these threats."

Microsoft
Public submission to the Cyber Security Strategy 2020

62 Certain businesses can reduce the number of threats entering Australia by automatically blocking known malicious content. This solution that will protect Australians and Australian businesses at speed and scale. Over the life of this Strategy, the Australian Government will support businesses to implement threat-blocking technology that can automatically protect citizens and businesses from known malware and trojans. The Australian Government will also consider how it can provide legislative and any other assistance to telecommunications providers implementing this technology.
As part of this initiative, the Australian Government will invest $12.5 million for the ACSC to provide Australia's major telecommunications providers with information about known malicious websites, malware, phishing campaigns and online scams to boost providers' ability to block threats at scale.
This funding will support industry partnership, research and development of new capabilities to detect and block threats at scale, reducing the volume of cyber threats impacting Australians so they can focus on running their businesses and building the economy. usinesses and building the economy.

Cleaner Pipes initiative

In May 2020, Telstra announced its Cleaner Pipes initiative, which upscales Telstra's Domain Name System (DNS) filtering, to automatically block millions of malware communications as they try to cross Telstra's infrastructure every week.
Telstra has been trialling this initiative for 12 months, including blocking the command and control communications of botnets and malware and stopping downloads of remote access trojans, backdoors and banking trojans. Cleaner Pipes complements similar initiatives focused on reducing malicious SMS and scam calls; Telstra currently blocks more than half a million scam calls per month from reaching customers. The Australian Government is working with businesses to support the roll-out of this solution to more Australians.

Securing products and services

63 Australians are connecting to the internet in more ways than ever before. By 2030, it is estimated that there will be more than 21 billion Internet of Things devices connected to the internet globally, with the highest estimations predicting over 64 billion devices.[5] This includes personal devices like smartwatches, fridges and baby monitors; health devices such as pacemakers and blood-glucose monitors; and industrial devices that can drive business efficiencies.

5 NortonLifeLock (2020), The future of IoT: 10 predictions about the Internet of Things, available at https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html; Business Insider (2020), A look at examples of IoT devices and their business applications in 2020, available at https://www.businessinsider.com/internet-of-things-devices-examples?r=AU&IR=T

64 To support businesses in taking action to protect themselves and their customers, the Australian Government will release the voluntary Code of Practice: Securing the Internet of Things for Consumers, to inform businesses about the cyber security features expected of internet-connected devices available in Australia. The 13 principles in the voluntary Code of Practice will signal to manufacturers the importance of protecting consumers. Adoption of the Code of Practice, together with associated guidance material produced by the ACSC, will benefit Australians and SMEs by increasing the number of secure products available for purchase. The Australian Government will provide consumers with information about what to take into consideration when purchasing Internet of Things devices.

65 Similar to steps taken in the United Kingdom, the Australian Government will co-design supply chain principles for decision makers and suppliers, to encourage security-by-design; transparency; and autonomy and integrity in investment, procurement and security. The Australian Government will build these principles into decision-making practices, supporting competition and diversity in the market. To keep guidance up to date as technology and threats continue to evolve, the Australian Government will continue to monitor and build on existing government initiatives that promote innovation in sovereign cyber security research and development. AustCyber is well placed to assure continued commercialisation and scaling of cyber security capabilities that support our nation's needs.

66 In making decisions about what products and services they purchase, consumers play an important role in encouraging businesses to build cyber security into their offerings. The Australian Government will continue to assess whether consumers have the information they need to make informed cyber security choices when purchasing products and services. If voluntary advice and guidance like the Code of Practice is not enough to drive change, then additional steps may need to be considered. The Australian Government will establish a Cyber Security Best Practice Regulation Task Force to work with businesses and international partners to consider options for better protecting customers by ensuring cyber security is built into digital products, services and supply chains. This reflects community expectations of product safety, and the risk of vulnerabilities spreading due to the increasing interconnection between devices.

Growing a cyber skilled workforce

67 A strong workforce of skilled cyber security professionals is a key enabler of Australia's digital economy and security. To support businesses in undertaking these actions, this Strategy includes a Cyber Security National Workforce Growth Program that will assist businesses and academia to grow the cyber skilled workforce of the future. Growing the cyber security skills pipeline will ensure all critical infrastructure owners and operators and businesses have greater access to skilled cyber security professionals with the right skills to meet demand. This complements the steps the Australian Government has already taken to invest in the growth of the Defence cyber workforce.

68 Greater opportunities will be provided to Australians seeking to train for a world-class career in cyber security. The Cyber Security National Workforce Growth Program will be underpinned by a $26.5 million Cyber Skills Partnerships Innovation Fund, which will encourage businesses and academia to partner together to find innovative new ways to improve cyber security skills. Activities that will be eligible under the Fund include:

- scholarships
- apprenticeships, or apprenticeship-style courses in higher education
- development and delivery of specialist cyber security courses for professionals
- retraining initiatives, to help existing professionals in other disciplines transition to cyber security roles
- training or professional development for teachers and board executives, including through practical partnerships or exchanges with industry
- internships, cadetships, work experience and staff exchanges
- digital training platforms and student delivered cyber security services
- any other innovative idea to meet the needs of businesses.

69 The Cyber Security National Workforce Growth Program seeks to grow cyber security skills at all stages of education, including primary, secondary and tertiary. It will inspire the next generation of cyber security experts and equip teachers to include cyber security in their classroom lessons. The ACSC will grow its education, skills, training, mentoring and coaching programs, including specialised programs for women who are still underrepresented in the sector. The Australian Government also intends to work with businesses and academia on the best way to ensure university courses meet employer needs, building on international examples. This includes considering how cyber security can be more consistently embedded in other disciplines, such as engineering and data science. Strengthening the links between government, businesses and the education sector is particularly important because of the speed of change in cyber security. Cyber security evolves much faster than other sectors, as technology changes and malicious actors adapt their tactics accordingly.

70 Businesses and the community need to have confidence in the cyber security industry. The Australian Government will continue to work with businesses on the best way to promote the cyber security profession and ensure there are clear professional standards for practitioners, and more consistency in the market for consumers. In the medium to longer term, this could involve exploring whether there is a need for cyber security accreditation frameworks, including how these would map against other existing licensing and professional accreditation frameworks. To provide consistency across the cyber security sector, this could be accompanied by professional competency requirements for maintaining accreditation. The Australian Government will work with businesses and international partners to understand if this would be valuable, and the best way for the cyber security sector to deliver and maintain these frameworks, including through close engagement with international partners.

> *"A globally competitive Australian cyber security sector will ultimately underpin the future success of every industry in the national economy."*
>
> **AustCyber**
> Public submission to the Cyber Security Strategy 2020

The cyber security sector offers diverse opportunities

Cyber security is one of the fastest growing sectors in Australia and worldwide. Its direct economic impact in 2019–20 is estimated at $15.7 billion in revenue, employing 19,475 people.[6] Rapid technological advancement and the evolving threat environment will continue to generate demand in the cyber security sector. AustCyber forecasts that almost 17,000 new jobs will be needed to 2026.[7]

The cyber security sector is vital to economic growth

Digital activity in 2019–20 directly contributed: $317 billion in gross output to the Australian economy; $105 billion (5.5%) to Australia's GDP; and 527,726 jobs to the Australian economy.[6] Cyber security enables the digital economy to grow and innovate, which is critical to Australia's prosperity and recovery from COVID-19, as more people and businesses move online to create and deliver services and goods.

Work from anywhere

Cyberspace is not bound by geography. Working in cyber security means that you do not have to be locked in to a single jurisdiction. Opportunities exist for Australian cyber security businesses to sell their solutions to offshore buyers and attract global investors.

Competitive wages

AustCyber's Cyber Security Sector Competitiveness Plan states that wages are high across the cyber security profession with a $12,000 average wage premium paid for a cyber security worker over an IT worker. Roles in management and leadership, and those that involve designing and building cyber systems, are currently commanding the highest salaries, with average wage premiums of more than $20,000 above general IT.[7]

You don't need to be an IT expert

One of the biggest misconceptions about a career in cyber security is that it requires a background in IT. Cyber security is a broad sector that encompasses technical roles, policy, risk management, marketing, engagement and more.

There are courses relating to cyber security available in every state and territory, with more than 850 courses available Australia-wide.

Further information on cyber security courses is available at: www.austcyber.com/educate/career-paths-and-opportunities

Sovereign capabilities benefit us all

The value of market diversity and certainty in supply chains has become more apparent than ever as COVID-19 has focused attention on the risk of over-reliance on single markets. This presents business opportunities for Australian sovereign cyber capability. In the wake of the COVID-19 pandemic, the Australian Government will continue to work with industry and academia to encourage the development of new sovereign Australian cyber capabilities and companies. The Cyber Security Cooperative Research Centre is uniquely placed to play a key role in helping governments and key stakeholders bring this Strategy to life by driving relevant and innovative research to build Australia's cyber security capacity and capability.

Interested in working in cyber security?

ASD is the Australian Government's eminent authority responsible for three critical missions, namely the collection of signals intelligence, offensive cyber actions and the strengthening of Australia's cyber security.

ASD offers entry level career opportunities through the ASD Graduate Program across almost every discipline. ASD also offers apprenticeships through the Australian Government Digital Apprenticeship Program for those who are looking for a new and exciting career, including students who are currently studying or have completed their year 12 certificate, people studying at a CIT or TAFE, and those with a passion for IT.

Further information is available at www.asd.gov.au/careers

6 AustCyber (2020), *Australia's Digital Trust Report 2020*, available at https://www.austcyber.com/resource/digitaltrustreport2020

7 AustCyber (2019), *Australia's Cyber Security Competitiveness Plan: 2019 Update*, available at https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019

Actions by the community

> *"An informed and educated consumer about the cyber threat landscape could be the most efficacious program that government could initiate."*
>
> **Cisco**
> Public submission to the Cyber Security Strategy 2020

71 Most cyber security incidents have an element of human error. This means it is critical that all Australians know how to stay secure online, especially as using new technology does not come naturally to everyone. This Strategy will empower Australians by providing the tools to do so in a secure way.

72 There are several things that Australians can, and should, do to be secure online. The ACSC will continue to provide best practice cyber security advice and assistance through the one-stop-shop cyber.gov.au. Cyber.gov.au provides all the information individuals need to know about being cyber secure and serves as an excellent foundation for further initiatives to build cyber security resilience within the community. Accessing and implementing this information are actions the community can take to increase their cyber security. In addition, there is growing private sector cyber security expertise that can assist in staying secure online across a range of services, such as the provision of anti-virus software to in-depth cyber security advice and response.

73 Through this Strategy, the Australian Government will build on existing advice to make sure messages about cyber security reach more Australians more often. The Australian Government will invest in a new public awareness raising campaign, delivered in coordination with campaigns about online safety (see the case study below). The Australian Government will also provide a comprehensive online cyber security training program for small businesses, older Australians and Australian families, delivered through cyber.gov.au.

What's the difference between online safety and cyber security?

As Australians spend more time online, they need to protect themselves from cyber threats and illegal and harmful content and behaviour.

Cyber security includes helping Australians to be secure online by protecting data, information, devices and networks from malicious actors. The ACSC, via cyber.gov.au, is the main point of contact for the public on cyber security.

Online safety includes protecting individuals, families, and communities from harmful content and behaviours such as cyber bulling, image-based abuse and illegal and harmful online content. The eSafety Commissioner, via esafety.gov.au, is the main point of contact for the public on online safety. With more Australians online as a result of COVID-19, the Australian Government has invested an additional $10 million to boost eSafety's investigations and support teams so help is available to Australians when they encounter harmful content and behaviours online.

The Australian Government recognises the need to provide clear and simple advice about how to be secure and safe online. Through this Strategy, Australian Government departments will work closely together to provide clear advice on both online safety and cyber security.
The Australian Government will also make it easier for businesses interested in both online safety and cyber security to engage with government.

74 Any Australian that needs cyber security advice or support should reach out to the experts as soon as they can. One of the main ways to get cyber security help is by contacting the ACSC's 24/7 hotline. Early action can prevent an incident, or reduce the harm if it has already occurred. The ACSC will receive more funding so this hotline can provide a greater number of services and increase its capacity.

75 Through this Strategy, the Australian Government will prioritise support to victims of cyber crime. Reporting cyber crime incidents through the ReportCyber website is an important way for the community to help us know the full extent to which cyber criminals are harming Australians. Being a victim of a cyber crime can be traumatic, but the impact can be reduced with the right help. Another way to get help is through the free specialist identity and cyber crime support service IDCARE. IDCARE is able to provide tailored, hands-on support to victims when they need it most. This Strategy will provide more funding to victim support services to help a growing number of people who need their assistance. By taking the above actions, government, businesses and the community will create a more secure online world for Australians, their businesses and the essential services upon which we all depend.

Tips to secure your Internet of Things device

The Australian community can take action to make informed purchasing decisions. Consumers should ask the following questions when purchasing internet-connected devices to reduce the risk of purchasing an insecure device.

Before purchasing an Internet of Things device

- Is the device made by a well-known reputable company and sold by a well-known reputable store?
- Is it possible to change the password?
- Does the manufacturer provide software updates?
- What data will the device collect and who will the data be shared with?
- Does the device do only what you want it to do?

Setting up an Internet of Things device

- Does the device need to be connected to the internet?
- Is the device in a secure location?
- Do I change the default username and password?
- Is my Wi-Fi network set up securely, and does it have a secure password?
- Are unnecessary device features turned off?

Further advice on how to stay secure online is available at cyber.gov.au.

This Strategy's work does not end here

Both government and businesses have finite resources. The actions outlined in this Strategy address the most urgent issues. Technology is constantly changing; measures designed to improve security in today's online world can be quickly overtaken by new technologies, systems, software and applications.

Australia cannot therefore set and forget, especially as technology and threats continue to evolve. The Australian Government will continue to work with businesses and the community to ensure that all continue to take actions to create a more secure online world for Australians, their businesses and the essential services upon which we all depend.

The standing Industry Advisory Committee (see 'Implementation and measuring progress') will play a key role in advising the Minister what specific actions to take as part of this Strategy in the longer-term.

The Minister will periodically update this Strategy's Action Plan (on the following pages) and report to the Australian Government and the community on measures to continually enhance Australia's cyber security.

Action plan

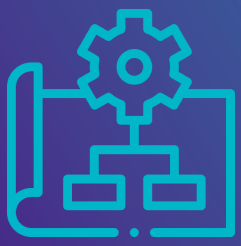
Initiative	Description	Who benefits?
Actions by governments		
Protect critical infrastructure in a national emergency	The Australian Government will introduce new laws to make sure Australia can recover quickly from a cyber security emergency. This will include providing reasonable and proportionate directions to businesses to minimise the impact of an incident and taking direct action to protect systems during an emergency.	– Australia's critical infrastructure and systems of national significance will be able to quickly recover in the event of a significant cyber incident. – All businesses and citizens will benefit from essential services being protected or restored as quickly as possible
Enhance incident response procedures	The Australian Government will invest $10.0 million for an expanded National Exercise Program that will bring Commonwealth, state and territory government agencies together with private sector organisations to plan and prepare for cyber security incidents. The Australian Government will also work with states and territories to expand standard cyber security incident procedures to formally recognise and plan for business contributions in responding to a major incident.	– Australia's critical infrastructure and businesses will be involved in national incident response procedures, improving their ability to recover. – The essential services that Australians rely on every day will be quickly restored in the event of a significant cyber incident.

Initiative	Description	Who benefits?
Bolster law enforcement capabilities, including on the dark web	The Australian Government will invest $124.9 million to strengthen law enforcement's counter cyber crime capabilities. This includes an investment of $89.9 million in the AFP to set up target development teams and bolster its ability to go after cyber criminals. This will be complemented by the use of the Australian Transaction Reports and Analysis Centre's specialist financial intelligence expertise to target the profits of cyber criminals. The Australian Government will ensure it has fit-for-purpose powers and capabilities to discover, target, investigate and disrupt cyber crime, including on the dark web. The Australian Government will invest over $31.6 million to extend and expand the ACSC's ability to counter cyber crime actors offshore and provide technical advice and assistance to Commonwealth, state and territory law enforcement agencies in identifying and disrupting cyber criminals. This builds on the Australian Government's $40.0 million countering foreign cyber criminals election commitment. Combined, these initiatives will enable government to take the fight to foreign actors that seek to target Australians.	– Cyber criminals will be deterred from targeting Australians, reducing the cost of cyber crime and strengthening the Australian economy. – Australians will be better protected from cyber crime.
Harden Australian Government IT	The Australian Government will strengthen defences of its networks by centralising their management and operation, including considering secure hubs. This centralisation seeks to reduce opportunities for malicious actors to target smaller agencies with less secure IT, and will increase opportunities to focus the Australian Government's cyber security investment. Standard cyber security clauses will be in government IT contracts. Australian government agencies will also put a renewed focus on policies and procedures to manage cyber security risks.	– Government IT systems, as systems of national significance, will be more secure. – Businesses and citizens will be confident that their data is more secure.
Improve threat information sharing	The Australian Government will invest $35.3 million through the ACSC to deliver a new partner portal coupled with a multi-directional threat-sharing platform. The Australian Government has also invested $1.6 million to enhance the cyber security of Australian universities. This will fund a threat intelligence-sharing network, sector-wide threat modelling and a national cyber security forum that will meet three times a year.	– Australia's critical infrastructure and businesses will have increased access to threat information, allowing them to better prepare for and defend against cyber threats. – Less sophisticated malicious cyber activity will be stopped before it reaches businesses and households.

Initiative	Description	Who benefits?
Uphold existing international law and norms of resposibility state behaviour in cyberspace	The Australian Government will deter malicious activity by imposing stronger consequences for those who act contrary to existing international law and agreed norms when it is in Australia's national interest to do so.	– Malicious nation states and state-sponsored actors will be deterred from targeting Australia's critical infrastructure and systems of national significance. – Australia as a whole will become a less desirable target for malicious state-based cyber activity, reducing the cost on our economy, and upholding our security and sovereignty.
Strengthen cyber security partnerships	The Australian Government will invest $67.9 million to expand the JCSC program. A broader range of ACSC staff and capabilities will be available to enhance collaboration with and support for state, territory and local governments, industry partners and academia across the country. The Australian Government will invest $8.2 million to establish a Department of Home Affairs presence at each JCSC to provide a whole-of-government approach to cyber security engagement.	– Australia's critical infrastructure, businesses and government agencies will have access to a collaborative forum to improve their cyber security practices.
Clarify cyber security obligations for Australian businesses	In line with advice from the Industry Advisory Panel and stakeholder feedback, the Australian Government will work with businesses on possible legislative changes that clarify the obligations for businesses that are not critical infrastructure to protect themselves and their customers from cyber security threats. This consultation will consider multiple reform options, including the role of privacy and consumer protection laws, and duties for company directors.	– Australian businesses will have clarity about what they have to do to protect themselves and their customers. – Consumers will have increased confidence in the security of products and services.
Stay ahead of the technology curve	The Australian Government will invest $118.0 million to expand its data science capabilities, ensuring Australia remains at the forefront of the technological advancements in cyber security. The Australian Government will also invest $20.2 million to establish cutting-edge research laboratories to better understand threats to emerging technology. Five hundred additional intelligence and cyber security personnel will be recruited at a cost of $469.7 million over 10 years. The Australian Government will invest $385.4 million to enable and enhance intelligence capabilities.	– Staying ahead of the technological curve will ensure Australia is able to adapt to emerging cyber security threats, improving national resilience and creating economic opportunities for Australia cyber security businesses.
Actions by businesses		
Improve baseline security for critical infrastructure	The Australian Government will implement minimum cyber security requirements for operators of critical infrastructure and systems of national significance. The Australian Government will also refine incident reporting for compromises and near-misses that meet a certain threshold. To complement this work and as part of the Australian Government's election commitment, the ACSC will receive $66.5 million to assist Australia's major critical infrastructure providers assess their networks for vulnerabilities and to enhance their cyber security posture. The Australian Government will also invest $62.3 million to deliver a national situational awareness capability to better enable the ACSC to understand and respond to cyber threats on a national scale.	– Australia's critical infrastructure and systems of national significance will be more secure. – All businesses and citizens that rely on critical infrastructure will benefit from continued access to essential services.

Initiative	Description	Who benefits?
Uplift the cyber security of SMEs	The $8.3 million Cyber Security Connect and Protect Program will equip trusted organisations like chambers of commerce and business associations to raise the cyber security of SMEs in their local area.	– Australia's economy will be strengthened and more resilient through the improved cyber security of SMEs.
Create a more secure Internet of Things	The Australian Government will release the voluntary Code of Practice on the security of the Internet of Things that will make the devices used by households and businesses more cyber secure.	– Internet of Things products in Australia will have improved cyber security, reducing costs on Australia's economy currently borne by device vulnerabilities. – Consumers will have greater access to secure Internet of Things devices, reducing their exposure to malicious cyber activity.
Grow a skilled workforce	The $50.0 million Cyber Security National Workforce Growth Program will grow the pipeline of skilled, trusted and job ready cyber security workers in business and government. The following four elements are included in the Program. A $26.5 million Skills Partnership Innovation Fund will create new opportunities for businesses and academia to partner on innovative skills projects that directly meet employers' skills needs. The ACSC will receive $6.3 million to grow its education, skills, training, mentoring and coaching programs, including specialised programs for women. The Australian Government will invest $14.9 million in Questacon, enabling it to design challenges and teacher training that prepare primary, secondary and tertiary students for a career in cyber security. $2.5 million will be allocated to enhanced data collection on the cyber security skills shortage. The Cyber Security National Workforce Growth Program complements the $40.0 million invested by the Australian Government as part of their election commitment to grow the Defence cyber workforce. These initiatives will be further strengthened by the Minister for Employment, Skills, Small and Family Business's announcement of new, fast-tracked training qualifications for the ICT sector to further equip Australia's workforce with cyber security and digital skills.	– Australia's critical infrastructure and businesses will have greater access to skilled cyber security professionals, strengthening their cyber security practices. – Australians will have new opportunities to train for a world class career in cyber security.
Block threats automatically	Over the life of this Strategy, the Australian Government will support businesses to implement threat blocking technology that can automatically protect citizens from known malicious cyber threats. The Australian Government will consider how it can provide legislative certainty to telecommunications providers implementing this technology. The Australian Government will also invest $12.5 million in new strategic mitigation and disruption options. This funding will support industry partnerships on, research into and development of new capabilities to detect and block threats at scale, to prevent malicious cyber activity from ever reaching millions of Australians.	– Australian businesses and households will benefit as threats are blocked before reaching them.

Initiative	Description	Who benefits?
Actions by the community		
Access guidance and information on cyber security	The Australian Government expects the community to act on best practice advice from the ACSC on how to be secure online. Under this Strategy, the Australian Government will continue to raise awareness about cyber security risks. The Australian Government will invest $4.9 million in a public awareness campaign targeting vulnerable Australians. The Australian Government will work with large businesses such as banks and internet service providers to ensure that SMEs have access to cyber security information in the normal course of running their business. The Australian Government will develop toolkits that SMEs can use to raise the cyber security awareness of their staff. The Australian Government will encourage big businesses to provide these toolkits to small businesses as part of a secure bundle of services. The ACSC will provide online cyber security training for SMEs, older Australians and families. This also complements the $10.0 million the Australian Government has invested to boost eSafety's investigations and support teams so help is available to Australians when they encounter harmful content and behaviours online.	– Greater community awareness will reduce the cost of malicious cyber activity for businesses and strengthen the Australian economy. – Greater community awareness will reduce the effectiveness of malicious cyber activity on Australian households, protecting families from harm.
Access help and support when needed	All Australians should access help and support if they are unsure about how to be secure online, or if they have been the victim of a cyber crime. The Australian Government will invest $58.3 million to enhance customer engagement channels and $12.3 million to extend the 24/7 cyber security helpdesk to SMEs and families. This will enhance the provision of cyber security advice and technical assistance to all Australians, improve the ReportCyber incident reporting tool, and provide additional online resources, and practical, tailored advice and information for all Australians. This also complements the Australian Government's $26.0 million investment to support the ACSC to expand its assistance to the SMEs and the community. The Australian Government will also provide $6.1 million to bolster services to victims of identity and cyber crime.	– Victims of cyber crime, including SMEs, will have greater access to support services to more effectively recover from an incident.
Make informed purchasing decisions	All consumers need to make smart cyber security decisions when purchasing digital devices. Through this Strategy the Australian Government will increase the amount of information available for consumers about what to look for when buying a product. This information will be available on cyber.gov.au. In the longer-term, the Australian Government will consider whether additional steps are needed to inform consumers, such as cyber security product labelling.	– Consumers will benefit by knowing what cyber security features to look out for when buying a digital device.



Implementation and measuring progress

76 The Australian Government recognises the importance of robust strategy implementation and evaluation arrangements for this Strategy.

77 The Minister for Home Affairs has primary responsibility for delivering this Strategy, with support from other ministers as required. A Cyber Security Strategy Delivery Board, led by a senior Home Affairs official, will be responsible for day-to-day implementation of this Strategy.

78 An Industry Advisory Committee will also be established to guide the implementation of this Strategy. The Industry Advisory Committee will provide ongoing advice about the best ways to address Australia's cyber security challenges, and will report directly to the Minister for Home Affairs. The Industry Advisory Committee will make public reports about the progress of this Strategy. This builds on the success of the Industry Advisory Panel that assisted in developing this Strategy.

Metrics

Initiative	How the Australian Government will measure success
Actions by governments	
Protect critical infrastructure in a national emergency	– Arrangements are in place for the Australian Government to respond to a cyber security emergency in a timely and effective manner. – There is increased visibility of threats to critical infrastructure and systems of national significance, with information available in near-real-time for those who need it to actively defend networks.
Enhance incident response procedures	– Updated Cyber Incident Management Arrangements outline how governments and businesses will increase their readiness to respond collectively to a significant national incident. – More government agencies and private sector organisations have strengthened their readiness and resilience.

Initiative	How the Australian Government will measure success
Bolster law enforcement capabilities, including on the dark web	– Through enhanced capabilities and coordination, the Australian Federal Police, Australian Criminal Intelligence Commission and the ACSC identify and disrupt more cyber crime targets. – Agencies have the authorities they need to discover, target, investigate and disrupt cyber crime and cyber-enabled crime. – More responses to online crimes are coordinated between the Australian Government, states and territories.
Harden Australian Government IT	– Centralisation of Australian Government IT networks makes it easier to defend against malicious activity.
Improve threat information sharing	– Government and businesses have increased visibility of cyber threats in near real-time. – There is increased two-way flow of cyber security information.
Uphold existing international law and norms of responsible state behaviour in cyberspace	– Australia's response to unacceptable behaviour in cyberspace aligns with international law and norms of responsible state behaviour in cyberspace. – A new Cyber and Critical Technology International Engagement Strategy is implemented.
Strengthen cyber security partnerships	– Customer experience survey data indicates effective partnerships between businesses and government.
Clarify cyber security obligations for Australian businesses	– Consultation is undertaken on possible future reforms to clarify cyber security obligations for Australian businesses.
Stay ahead of the technology curve	– The Australian Government has sovereign research capability to assess vulnerabilities in emerging technology.
Actions by businesses	
Improve baseline security for critical infrastructure	– There are clear cyber security requirements for critical infrastructure providers regardless of ownership arrangements. – Government has timely access to information about cyber security incidents and near-misses. – Critical infrastructure providers are supported to improve their cyber security.
Uplift the cyber security of SMEs	– An increasing number of small businesses are improving their cyber security practices.
Create a more secure Internet of Things	– Businesses have a better understanding of best practice security controls for the Internet of Things.
Grow a skilled workforce	– Survey data indicates increasing availability of job ready cyber security workers. – Businesses and academia develop innovative programs to meet local cyber security skill requirements. – More primary, secondary and tertiary students are inspired to pursue a career in cyber security.
Block threats automatically	– More known malicious threats are prevented from reaching Australians.

Initiative	How the Australian Government will measure success
Actions by the community	
Access guidance and information on cyber security	– Reach and behaviour change metrics for awareness campaigns indicate that effective guidance has been delivered. – The Agency Heads Committee on Online Safety Number oversees a number of campaigns.
Access help and support when needed	– Increased availability and quality of support services for victims of cyber crime. – Increased availability of cyber security advice and assistance for all Australians, including through the ACSC's expanded 24/7 helpdesk.
Make informed purchasing decisions	– Community awareness of how to purchase secure digital products and services.
Report cyber crime	– Increased understanding of the impacts of cyber crime on the community.