Australia's Cyber Security Strategy 2020

Cyber Security Industry Advisory Committee Annual Report 2021

© Commonwealth of Australia 2021

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

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

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

Contact us

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

Cyber, Digital and Technology Policy Division
Department of Home Affairs
4 National Circuit Barton ACT 2600
cybersecuritystrategy@homeaffairs.gov.au

Australia's Cyber Security Strategy 2020

Cyber Security Industry Advisory Committee Annual Report 2021

Table of Contents

Chair's Foreword

With the world well into the grip of a global pandemic, doing things digitally is part of our daily life more than ever before. While engaging digitally allows us to thrive, it also increases opportunities for those who seek to do us harm online to do so.

Input and perspectives from industry and academia in the delivery of Australia's Cyber Security Strategy 2020 (the Strategy) is critical to strengthening Australia's overall cyber resilience, and that has been the task of the Cyber Security Industry Advisory Committee (the Committee) over the last 9 months. Since the Committee was established in October 2020, the digital world and the cyber threat environment has continued to evolve. Important developments during this time included the launch of the Australian Government's Digital Economy Strategy targeting Australia to be a globally leading digital economy by 2030, and further investments by the Government to support and strengthen cyber defences. The Government has also launched its International Cyber and Critical Technology Engagement Strategy through which it engages with global likeminded nations in the joint effort to manage cyber risks.

The changing threat environment and the evolving nature of technology means that there has never been a more important time for Government and industry to work together. This needs to address cyber threats targeting the full spectrum of our society, critical infrastructure to businesses, and our families. As a Committee, we are privileged to help shape the initiatives that are being progressed under the Strategy.

One of Australia's fastest growing threats is ransomware and I am pleased the Committee's first public thought piece, *Locked Out: Tackling Australia's ransomware threat* focused on this important topic. The paper is an important contribution to helping Australian businesses understand the risk of ransomware and prepare accordingly.

This annual report from the Committee demonstrates how industry and the Australian Government continue to work together to protect all Australian's from cyber security threats and our views of important areas of focus over the next 12 months. I thank all Committee members for their support and advice.

Andrew Penn
Chair of the Cyber Security Industry
Advisory Committee
Chief Executive Officer of Telstra

Introduction

This annual report provides an update on the Committee's work since its establishment on 20 October 2020. It delivers key information to:

1. Outline progress on the implementation of the Strategy;
2. Highlight the Committee's advice to Government and how this has shaped the implementation of the Strategy;
3. Provide an overview of the current cyber threat environment; and
4. Provide the Committee's views on emerging cyber security policy issues and priorities.

Over the lifetime of the Strategy the Committee will support Government with industry-based advice to ensure Australia is in a position to meet the evolving cyber challenges that are key to our nation's economic prosperity and national security.

The Strategy at a glance

On 6 August 2020, the Government released Australia's Cyber Security Strategy 2020 and a $1.67 billion package to help protect Australians from cyber security threats. The Strategy succeeds and builds on Australia's 2016 Cyber Security Strategy, which set out the Government's four-year plan to advance and protect our interests online and was supported by a $230 million investment.

To develop the Strategy, the then Minister for Home Affairs, The Hon Peter Dutton, MP, established a Cyber Security Strategy Industry Advisory Panel (the Panel) to provide strategic advice and guidance. In July 2020, the Panel released their final report with 60 recommendations for Government, industry and individuals in the community to build Australia's cyber defences.

The Government adopted the overwhelming majority of the Panel's recommendations to develop the Strategy to achieve a more secure online world for Australians, their businesses and the essential services upon which we all depend.

Key initiatives under the Strategy are:

- establishing cyber security minimum standards for key critical infrastructure sectors and systems of national significance;
- enhanced cyber security capabilities for the Australian Signals Directorate (through the Cyber Enhanced Situational Awareness Response package);
- strengthening Australia's counter cybercrime capability (including investing in the Australian Federal Police);
- growing Australia's cyber security skills and workforce;
- supporting small and medium enterprises (SMEs);

- enhancing the cyber security of academic institutions;
- increased cyber security awareness and victim support for Australian families, households and small to medium enterprises; and
- hardening Government agencies' own cyber defences.

New cyber security initiatives

Since the launch of the Strategy in August 2020, the Government has announced a range of new initiatives that support Australia's cyber security and underpin our digital economy.

In October 2020, the Government released the Modern Manufacturing Strategy, investing around $1.5 billion to make Australian manufacturers more competitive, resilient and able to scale-up to take on the world. Enabling technology, such as cyber security, will help Australian manufacturers scale-up and become more competitive and resilient.

In April 2021, the Government released Australia's International Cyber and Critical Technology Engagement Strategy, outlining a vision for a safe, secure and prosperous Australia, Indo-Pacific and world enabled by cyberspace and critical technology. This strategy guides Australia's practical international engagement across cyber and critical technology issues, in order to create an environment that embraces the enormous opportunities of innovation while avoiding and mitigating the risks.

In May 2021, the Government released the Digital Economy Strategy, investing almost $1.2 billion to grow Australia's future as a modern and leading digital economy by 2030.

The Digital Economy Strategy expands Cyber Security Strategy 2020 funding by $43.8 million to further grow Australia's cyber security skills and workforce. It also includes a range of new measures to promote cyber security, safety and trust, including:

- securing 5G and future 6G connectivity;
- ensuring the security of Australian Government data;
- underpinning the digital environment with trusted identity;
- Digital Skills Cadetship Trials; and
- Next Generation Technology Graduates Program (for emerging technologies, which may include cyber security technologies).

The Government has also committed $4.9 million to strengthen cyber security capability in the energy sector:

- expand the Australian Energy Sector Cyber Security Framework to include the gas sector;
- deliver the 2020-21 Australian Energy Sector Cyber Security Framework cyber security assessment program for the electricity and gas sectors, in partnership with the Australian Energy Market Operator. This includes a facilitation program to support first-time participants;
- deliver a cyber security exercise to test response protocols and arrangements; and
- review cyber incident response arrangements and emerging cyber security vulnerabilities in the energy sector.

The Industry Advisory Committee

The Strategy recognised the value of an industry-led Panel and sought to ensure valuable contributions from industry leadership continued.

On 20 October 2020, the then Minister announced the establishment of the Cyber Security Industry Advisory Committee to provide independent strategic advice on Australia's cyber security challenges and opportunities to help guide the Strategy as it enters the implementation phase.

The Committee comprises the members listed below. Additional details on the Committee members are included in Appendix A.

- Andrew Penn, Industry Advisory Committee Chair, Chief Executive Officer of Telstra (former Chair of the Industry Advisory Panel)
- Cathie Reid, Industry Advisory Committee Deputy Chair, Chair of AUCloud
- Darren Kane, Chief Security Officer of NBN Co (former Industry Advisory Panel Member)
- Chris Deeble AO CSC, Chief Executive of Northrop Grumman Australia (former Industry Advisory Panel Member)
- Bevan Slattery, Chairman of FibreSense
- Corinne Best, Trust and Risk Business Leader of PricewaterhouseCoopers Australia
- Patrick Wright, Group Executive Technology and Enterprise Operations NAB
- Rachael Falk, Chief Executive Officer Cyber Security CRC
- Professor Stephen Smith, Chair of Advisory Board, University of Western Australia Public Policy Institute
- David Tudehope, Chief Executive Officer, Macquarie Telecom Group

The Committee welcomes the opportunity to contribute to robust and effective cyber security outcomes for Australia and is pleased to publish its first annual report.

The Strategy's implementation progress

The Committee provided guidance to the Government on implementation of the Strategy during its first year. This section provides a summary of progress for key initiatives progressed as part of the Strategy's implementation. A more detailed account of the Strategy's progress can be found in Appendix B.

Since its launch in August 2020, the Government has sought to establish a legislative and policy foundation which can support the further development of initiatives over the life of the Strategy.

Governance and evaluation mechanisms

Governance and oversight is a key priority to ensure the Strategy's progress is tracked, evaluated, and risks are managed.

The following governance bodies have been established or given specific oversight functions to oversee and/or provide advice on the Strategy's implementation:

- the Industry Advisory Committee;
- the Interdepartmental Committee on Cyber Security. A Commonwealth Deputy Secretary-level committee focused on strategic coordination across Government; and
- the Cyber Security Strategy Delivery Board. A Commonwealth senior executive board focused on inter-agency coordination and implementation of programs.

An Evaluation Approach has been established for the Strategy, providing a framework to guide the consistent, robust, and transparent evaluation of outcomes and performance of the Strategy and its constituent components.

The Evaluation Approach sets out the principles that will be applied to all evaluation activities under the framework, as well as an evaluation hierarchy that translates between the metrics and outcomes identified in the Strategy, and the more specific program level measures required to monitor the effective implementation of the Strategy.

This Evaluation Approach is intended to enable Government to allocate responsibility for evaluation and reporting under the Strategy in a consistent manner, making use of existing evaluation mechanisms within agencies rather than duplicating effort. These evaluation responsibilities have also been mapped against the Strategy's governance structures, differentiating between internal Government performance evaluations, security classified elements, and public accountability of what outcomes have been achieved under the Strategy and their impact on Australia.

The Committee considers there is merit in the development of a dashboard to track the nation's performance in keeping Australians safe in the digital world, and the overall maturity of our cyber capabilities.

Critical Infrastructure and Systems of National Significance

After consultation with industry, the Security Legislation Amendment (Critical Infrastructure) Bill 2020 was introduced into Parliament on 10 December 2020.

Government worked with the Committee, industry peak bodies, existing regulators, state and territory governments, and critical infrastructure entities to scope the remit and framework for the reforms.

The Department of Home Affairs engaged across two phases of consultation between August and November 2020. Consultation revealed broad in-principle support for the critical infrastructure and systems of national significance legislative reforms, but the relatively short duration of consultation also highlighted areas for further consultation in the detailed design of regulations for each sector.

The Government took on board comments and introduced the Security Legislation Amendment (Critical Infrastructure) Bill 2020 into the Australian Parliament. This Bill is currently before the Parliamentary Joint Committee on Intelligence and Security for inquiry.

> *Over 3000 individuals were consulted in the development of the critical infrastructure and systems of national significance reforms.*

Government is currently undertaking a staged, sector-by-sector approach to co-design requirements to minimise regulatory burden and duplication with existing regulatory frameworks. Finalisation of the rules will be undertaken progressively following passage of the legislation by Parliament.

Bolstering law enforcement capabilities

The Government is developing the next National Plan to Combat Cybercrime in consultation with state and territory governments.

The National Plan will consolidate a national framework to bring together the powers, capabilities, experience and intelligence of all of Australia's jurisdictions to build a strong operational response to cybercrime. The National Plan will also focus on strengthening public-private partnerships, and providing better support to the victims of cybercrime.

The Government has announced a $89.9 million investment to expand the Australian Federal Police's (AFP) multi-disciplinary cybercrime investigation teams across Australia. These teams are comprised of investigators, intelligence analysts and technical specialists. The expansion will support the AFP's operational capabilities to identify, disrupt and investigate cybercrime with the aim of making Australia a more costly environment for cybercriminals.

The AFP has continued to build coordinated and collaborative local, national and international policing efforts to counter the increase in cybercrime and cyber threats.

> *1 in 3 Australian adults were impacted by cybercrime in 2019.*[1]

[1] NortonLifeLock (2020), 2019 Cyber Safety Insights Report Global Results

Enhancing collaboration to tackle cyber threats, the Australian Cyber Security Centre (ACSC) has integrated law enforcement agencies including the AFP and the Australian Criminal Intelligence Commission (ACIC), to enhance Australia's response to cyber threats. The ACSC has also undertaken offensive cyber operations to disrupt criminals offshore.

Through this cooperation, and with other partners, the Australian Signals Directorate (ASD) has undertaken a number of offensive cyber activities. This includes working with partners to target cybercriminals selling credit card details on the dark web, resulting in the prevention of potential losses of over $7.5 million to Australians and $90 million globally.

ASD also assisted in the removal of over 6000 websites hosting cybercriminal activity, and disabled infrastructure of offshore criminals responsible for stealing money and data from Australians during the COVID-19 pandemic.

The Government introduced the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 into Parliament in December 2020. It proposes 'fit-for-purpose' powers and capabilities to discover, target, investigate and disrupt cybercrime, including on the dark web. The Bill is currently under consideration by the Parliamentary Joint Committee on Intelligence and Security.

Improve threat information sharing

ASD has commenced work to co-design enhancements to cyber threat intelligence sharing with a range of industry and government partners, including the telecommunications, financial services, energy, cloud and defence industry sectors.

ASD has also piloted a Protected Domain Name Server (DNS) service for government agencies, which blocks known 'bad' domains or malicious actors. This has prevented a range of threats. ASD has also continued to expand use of host based sensors at Government agencies to monitor for threats, with over 36,000 sensors deployed.

> *The pilot Protected DNS Service has serviced over 1 billion queries and blocked over 125,000 threats.*

Over 20 companies have agreed to participate in the Cleaner Pipes initiative, including major banks, major telecommunications providers, major retail chains, and insurance providers. Collectively, the initiative is exploring capabilities to detect and block threats at scale, reducing the volume of cyber threats impacting Australians.

Telstra has already launched a number of Cleaner Pipes initiatives, and with the National Australia Bank have taken leadership roles, driving discussions to consider how to effectively implement threat blocking at scale across the range of participants.

The Government is supporting industry-led discussions between Australian stakeholders and domain registrars across the international community to identify processes to support faster blocking of cyber threats at the domain level. Government and industry are also currently discussing regulatory barriers to threat blocking, ahead of giving consideration to policy options to better support industry to protect Australians.

Support to victims of cybercrime

In January 2021, the Government signed a contract with IDCARE to provide up to $6.1 million to support Australian victims of identity theft, scams and cybercrimes by providing specialist support to recover from and minimise the impact of these incidents. The funding will be provided over four years, enabling IDCARE to deliver increased support services to victims, and provide Government with regular reporting on emerging threats and identity exploitation trends.

> *9226 cases were referred to IDCARE by the Commonwealth Government within the first five months of the contract.*

A cyber skilled workforce

Programs supporting the growth of Australia's cyber security skills availability have been progressed by the Government under the Cyber Security National Workforce Growth Program.

In February 2021, the first round of grants was announced under the Cyber Security Skills Partnership Innovation Fund. The fund provides industry and education providers with funding to deliver innovative projects that meet local requirements to quickly improve the quality and quantity of cyber security professionals in Australia.

> *Eight successful applicants were awarded a combined total of $8.2 million in the first round of grants under the Cyber Security Skills Partnership Innovation Fund.*

Identifying the importance of industry and education to work together on innovative projects to address workforce shortages and support growth of Australia's digital economy, Prime Minister Scott Morrison announced a $43.8 million expansion of the fund in May 2021.

The Australian Defence Force (ADF) Cyber Gap Program received 1009 applications for the 2021 year intake. Following a competitive selection process, 271 applicants were selected and will complete the program in December 2021.

The ACSC also progressed a number of cyber workforce initiatives, including sponsoring the Australian Women in Security Network Mentoring Pilot with 75 participants in 2021.

Joint Cyber Security Centres

As part of the Strategy and in recognition of the Industry Advisory Panel's recommendations regarding enhanced engagement with industry, the ACSC has undertaken a range of work to improve Joint Cyber Security Centres' (JCSC) capability and maturity including: expansion of the workforce (including Home Affairs outreach officers), upgrades to ICT and facilities, tiering of the ACSC's partnerships program, and investment in new services such as the work to co-design enhancements to the Cyber Threat Intelligence Sharing (CTIS) portal.

Over the last year, ACSC has continued to grow its JCSCs. In cooperation with the Northern Territory Government a new JCSC outreach office has been established in Darwin, improving support to businesses in the Northern Territory.

Throughout 2020 and 2021, ACSC's JCSCs continued to offer tailored support to industry and government partners. Over 200 events have been held either virtually or in the JCSCs in the first six months of 2021. These events included highly sensitive briefings on cyber threat intelligence to stakeholders in a number of critical industry sectors.

The ACSC also hosts partners from the Cyber Security Research Centre at the Sydney JCSC to support and promote deeper research on challenging cyber security issues facing the economy. In addition, the JCSCs supported a cyber security exercise that enabled an Australian state to exercise their own cyber practices in response to a critical incident.

Supporting SMEs

The ACSC Partnership Program has been expanded to support a broader range of stakeholders, including the introduction of a new 'Business Partner' tier available to Australian entities with a valid Australian Business Number (ABN). This tier provides organisations with access to ACSC products that help to build their understanding of the cyber security landscape, and provides advice on the steps required to protect themselves from cyber security threats.

> *Between May 2020 and May 2021, the ACSC published 30 new technical cyber security guides tailored for small businesses and individuals.*

Continuing the Strategy's commitment to strengthen industry partnerships, the Department of Home Affairs is rolling out a network of 15 cyber security outreach officers to bolster industry engagement across Australia, particularly focussed on SMEs.

The outreach officer network is focused on engaging with businesses at scale to maximise impact, operating as part of ACSC's JCSCs. The network will use peak bodies to serve as a conduit to not only inform industry of Commonwealth initiatives, programs and advice, but also to receive feedback on the needs of businesses.

Five Home Affairs outreach officers have commenced with the remaining officers to be onboarded over 2021-22.

In October 2020, the Government launched the Cyber Security Business Connect and Protect Program supporting 14 trusted organisations across Australia with $6.9 million in funding to deliver advice, and uplift cyber security resilience for an estimated 600,000 SMEs. As part of the program, the Government also released a Cyber Security Assessment Tool[2] in March 2021. The tool is available for all businesses to assess their current state of cyber security maturity and be provided with recommendations for action.

> *The Cyber Security Business Connect and Protect Program announced in April 2021 that $6.9 million in funding is being provided to 14 trusted organisations, uplifting cyber security resilience for an estimated 600,000 SMEs.*

As part of the Strategy, the Government is exploring options to uplift cyber security across the digital economy. In particular, the Government is considering the role of privacy, consumer protection laws and corporate governance as part of these options.

In considering how to assist Australian businesses to become more resilient to cyber security threats, the Government has consulted with the Industry Advisory Committee to ensure that any options considered are consistent with the views of industry and advice received through the Industry Advisory Panel Report.

The Government is also conscious of the need to carefully consider the regulatory burden of any option being considered, and will engage industry through public consultation to inform the development of possible options.

Enhance incident response procedures

Between 1 June 2020 and 31 May 2021, the ACSC responded to 1786 cyber security incidents, many of these affecting essential services including electricity, water, education, banking and finance, health, communications and transport.

[2] https://business.gov.au/news/is-your-business-cyber-secure

> *There has been a 400% increase in calls to the ACSC's 24/7 cyber hotline in May 2021 compared to May 2020.*

The ACSC supports Australian businesses and organisations by providing timely and updated advice on cyber security incidents, including advice in relation to Microsoft Exchange and SolarWinds vulnerabilities. This has included partnering with industry sectors, such as the banking and telecommunications sectors, who have helped augment ACSC's advice to a broad range of stakeholders on mitigating key vulnerabilities.

The Government is also developing greater cyber security preparedness and mitigation strategies across both government and industry domains. In 2020-21, the ACSC led work with Commonwealth agencies, industry, and state and territory governments to prepare for a national exercise on water and waste water that will be held in August 2021 – known as AquaEx Australia.

Awareness raising

Since the Strategy's launch, Commonwealth agencies have continued to improve coordination for cyber security and online harms messaging to the community. Providing the public with clear and consistent advice on how to be more secure online is a key initiative within the Strategy.

The Commonwealth has developed an Online Harms Communications Framework, drawing together a set of principles for Government to consider when developing or distributing public messages about online harms, including cyber security. The framework establishes a coordination mechanism to ensure consistency of messaging, and Government is encouraged to apply the Framework's principles and practices when planning leadership messages, organising major media engagements, undertaking advertising campaigns, responding to online crisis events and delivering education and awareness raising initiatives.

In December 2020, the ACSC commenced its 'Act Now, Stay Secure' campaign with a focus on ransomware. The awareness campaign targeted tailored security advice to the general population and SMEs. The initial focus provided information on how to prevent and recover from ransomware. Since then, the campaign has also provided advice on the importance of back-ups; ensuring strong passwords; and using multifactor authentication.

A Cyber Security Awareness Raising Campaign is currently in development by the Government, and will be launched in 2021-22.

International Cyber and Critical Technology Engagement Strategy

On 21 April 2021, the Minister for Foreign Affairs launched the International Cyber and Critical Technology Engagement Strategy. The international strategy aims to strengthen national security, protect Australia's democracy and sovereignty, promote economic growth, and pursue international peace and stability.

The international strategy complements the Cyber Security Strategy and other government initiatives to produce a cohesive domestic and international approach to developing cyber resilience and tackling issues of cross-border cyber threats.

Action is underway across the full range of objectives set out in the International Cyber and Critical Technology Engagement Strategy, covering Australia's values, security and prosperity. Since the launch of the international strategy, there has been progress in the reaffirmation of international law and norms of responsible state behaviour in cyberspace. The UN Group of Governmental Experts on Cyber agreed by consensus a report which for the first time confirms the application of international humanitarian law (the law of war) in cyberspace and provides practical guidance on the implementation of the agreed norms.

Australia has also deepened its relationships with partners in the Indo-Pacific on cyber security matters. This includes commencing new work under the Cyber and Critical Technology Cooperation Program on technology standards in Southeast Asia, and working with the United States, India and Japan in the context of a new Quad working group on Critical and Emerging Technology.

An overview of all of the Government initiatives supporting cyber security can be found in Appendix C.

The Committee’s work

The Committee provides the Minister for Home Affairs with considered advice on the development of cyber security policy and implementation of the Strategy from an industry and academic perspective.

The Committee formally met five times between October 2020 and July 2021, and participated in an additional four deep dives into the following areas: strategy implementation, cybercrime, workforce readiness, and JCSCs. These deep dives were conducted to enable further exploration of important and complex issues.

The Committee has helped shape several key initiatives under the Strategy. These include the development of the Security Legislation Amendment (Critical Infrastructure) Bill 2020, reforms under consideration by the Best Practice Regulation Taskforce, and the Government’s cyber security awareness campaign.

The Committee has considered the implementation of the Strategy, informed by briefings from relevant Government departments and the deep dive discussions. These considerations have taken into account the evolving cyber threat environment, the interests of industry and the community, and the use of policy and legislation to achieve the objectives of the Strategy for all Australians.

Committee’s advice on cyber security issues over the year

The Committee provided advice and perspectives to the Minister on a number of key cyber security issues, including:

- reforms to protect critical infrastructure and systems of national significance;
- initiatives to support small businesses and consumers;
- emerging cyber security trends and threats and impacts on businesses, with a focus on ransomware;
- whole-of-economy reform undertaken by the Cyber Security Best Practice Regulation Taskforce;
- raising cyber security awareness of families and businesses;
- best practices in cyber security, cybercrime and related fields;
- the changing nature of Australia’s workforce and the new challenges this brings to cyber resilience; and
- Government and industry collaboration through the ACSC’s JCSCs.

Ransomware thought-piece

The Committee's first public thought-piece was published on 10 March 2021 with a focus on ransomware. It urges Australians and their businesses – no matter how big or small – to strengthen their cyber defences and protect themselves from cyber threats.

A working group within the Committee was established (comprising Ms Cathie Reid, Ms Rachael Falk, Ms Corinne Best, Telstra, NAB, PricewaterhouseCoopers, Home Affairs and the ACSC), to develop *Locked out: Tackling Australia's ransomware threat*.[3]

The paper is aimed at helping individuals and businesses understand Australia's ransomware threat landscape, and was developed from real life case studies drawn from contributing Committee members, global research, and Australian Government threat briefings.

The paper considers:

- the change in the threat actor business model;
- the impact of weak controls or outdated software;
- the role of strong foundational controls;
- the impact attacks can have on SMEs, and essential steps they can action themselves to protect their organisation;
- whether cyber insurance is escalating attacks;
- the legality of ransomware payment;
- the role and obligations of directors; and
- the disclosure obligations on listed companies.

Reforms to Protect Critical Infrastructure and Systems of National Significance

The Committee provided advice to the Minister for Home Affairs on the Security Legislation Amendment (Critical Infrastructure) Bill 2020.

The Committee's feedback on the Exposure Draft of the Bill included several recommendations on key issues for consideration by the Government.

The Committee's recommendations primarily focused on: ensuring the Act continued to embed ongoing consultation and co-design with industry; amending the role of board members in approving the Critical Infrastructure Risk Management Program; reducing regulatory duplication; clarification of Government Assistance intervention powers; and considering the future inclusion of other assets in critical sectors.

The Government considered the Committee's feedback, which is reflected in the Bill which:

- implements Risk Management Programs by co-designing sector specific requirements with industry peak bodies and critical infrastructure entities throughout 2021;
- streamlines the role of boards in approving the Risk Management Program;
- clarifies mechanisms to avoid regulatory duplication;
- includes a range of protections to ensure the appropriate operation of Governance Assistance measures; and
- the regime allows for additional assets to be prescribed or declared as critical infrastructure assets where appropriate.

The Committee looks forward to working with Government on the ongoing co-design of sector specific requirements throughout 2021-22. The Committee will continue to work with Government and industry to ensure the legislation effectively protects the assets on which our society depends.

[3] https://www.homeaffairs.gov.au/cybersecurity/

Cyber security awareness raising

The Committee provided advice to Government on raising cyber security awareness, including through a public national cyber security awareness raising campaign.

The $4.9 million awareness raising initiative outlined in the Strategy is currently in development.

The Committee's advice included the use of social media to tailor messages and amplify the campaign for small businesses to ensure they know how to protect their data, and that of their customers. Further, the Committee notes in order to ensure effective cyber security uplift of individuals, Government needs to provide the public with clear and consistent advice on how to be more secure online. Awareness raising is a critical aspect of Australia's cyber security uplift.

The Committee has also advised Government that it considers further funding for awareness raising is warranted.

In response to the Committee's advice, some of the draft campaign messaging was further nuanced to better target the Government's intended audience. Government is designing the campaign to complement and align other government messaging, in particular online safety. The messaging directs people to the ACSC's cyber.gov.au, establishing it as a one stop shop for trusted advice and practical assistance.

A cyber security skilled workforce

The Cyber Security Skills Partnership Innovation Fund provides industry and education providers with funding to deliver innovative projects that meet local requirements to quickly improve the quality or availability of cyber security professionals in Australia.

Two Committee members provided support to review applications submitted under round one of the Strategy's $26.5 million Fund, including advice to ensure the program was sufficiently focussed on increasing the number of cyber security-skilled professionals, as balanced against the focus on innovation.

The Committee notes three distinct categories of 'need' in digital and cyber upskilling: cyber security literacy for all workers and individuals; cyber-capable workers involved in IT system builds and maintenance, including some identification and prevention of threats; and deep technical cyber security skilled workers, including in systems architecture and responding to complex cyber incidents.

The Committee supported the 2021 Targeted Update to the Australian and New Zealand Standard Classification of Occupations (ANZSCO), advocating for the inclusion of cyber security related occupations to reflect a modern Australian workforce.

Countering cybercrime

The Committee provided advice to Government on current efforts to counter cybercrime, in particular on the development of the National Plan to Combat Cybercrime. The Committee provided an industry perspective and further insight to Government on approaches law enforcement agencies could take to build on the success of existing public-private partnerships.

It was emphasised by the Committee the importance of Government leveraging industry to share skills, intelligence, and insights on emerging cyber threats, enabling the partnership to more rapidly respond and minimise harm to the community.

The Committee supports ongoing collaboration with Government to develop the National Plan.

Developments in the threat environment

The Committee's view of the threat environment is that Australia remains a target of both state-sponsored and criminal actors, whose malicious cyber activities were not hampered by the pandemic. These actors employed a wide range of capabilities to target Australian networks, seeking to extort money from organisations, or access sensitive information that could be used to weaken Australia's competitive advantage and degrade our national security.

Increasing use of ransomware

Ransomware has established itself as one of Australia's fastest growing cybercrime threats.

> *In May 2021, the ransomware attack on Colonial Pipeline, which carries almost half the fuel supplies to power the east coast of the United States, resulted in the company's decision to shut down the pipeline.*

Criminals' combined ability to exfiltrate sensitive data and encrypt networks – known as 'double extortion' – can result in severe operational, financial and reputational consequences for organisations, and large-scale data leakage for customers.

Widespread data encryption is not the sole method used to coerce payment, with cybercriminals now also stealing sensitive data – including employee and client personal information – and then threatening to release it publicly as an additional incentive for the victim to pay.

Victims are most likely to pay a ransom when they perceive it to be the best option for recovery. However, cybercriminals share information and when they are successful at extracting ransomware payments from victims not only does it re-incentivise them, but also attracts and motivates others, increasing Australia's attractiveness as a target.

There has been a noted shift for top tier cybercriminals to target their ransomware efforts towards entities they perceive as high profile, high value, and/or provide critical services. This pattern shifts away from prior experience of indiscriminately targeting large volumes of small-scale victims. However, smaller criminal groups are still widely using broad and indiscriminate tactics that impact individuals, and SMEs.

When deployed against essential services or critical infrastructure, ransomware may have rapid and serious consequences for the Australian community.

> *In August 2020, the New Zealand Stock Exchange was hit by multi-day distributed denial of service (DDoS) attacks. The perpetrators demanded payment of USD200,000 in bitcoin while tying up an estimated NZD34 billion in capital.*

The growing 'cybercrime-as-a-service' industry is making ransomware more accessible to a broader range of offenders. Criminals with limited technological skill can purchase and deploy bespoke ransomware variants or join affiliate programs that lease particular ransomware in return for a share of the ransom.

Cybercrime-as-a-service also increases the challenge in identifying, and attributing the use of some ransomware variants to specific actors or groups.

Business email compromise

Business email compromise (BEC) is an increasing and persistent threat worldwide. In Australia, BEC reporting has identified a recent increase in both frequency and impact. It is estimated to cost the Australian economy hundreds of millions of dollars each year. While instances of BEC are also almost certainly underreported, the AFP advised $149.8 million was lost to BEC by Australians in 2019-20.

> *Since January 2020, over 2100 incidents of BEC have been reported to ReportCyber with 1083 resulting in financial loss.*

Cybercriminals conducting BEC activity took advantage of the COVID-19 pandemic to exploit societal concern and used it as a theme for their phishing activities. For example, through theming their phishing campaigns with COVID-19 messaging, for very little extra effort, they were able to increase the likelihood of victims interacting with malicious content. The majority were relatively low value, unsophisticated attempts targeting individuals, SMEs and other organisations.

More sophisticated BECs, however, have resulted in many millions of dollars lost. In March 2020, a Victoria-based investment company lost $16.9 million after an employee had their email account compromised.

In the last four years, BEC groups have become more sophisticated and organised, developing enhanced and streamlined methodologies. Cybercriminals monitor email traffic, learning about their targets, and determining the most lucrative time to launch the scam. Individuals, such as senior executives, CEOs and chairs of boards, have been targeted and can sometimes be underprepared and unaware of how to best manage their personal digital environment to protect themselves and their organisations. This not only increases the likelihood of success but also increases the overall profit-margin.

Increased targeting of the supply chain

Malicious actors increasingly view the supply chain – including software, services and entities connected to businesses – as a priority target, and a vector for compromise. Targeting one weaker element of the supply chain can afford 'back door' access to a priority target and/or provide access to all customers of that entity.

Vulnerabilities in popular products or services can allow malicious cyber actors to compromise large numbers of organisations across multiple sectors. This makes the supply chain an even more enticing target. Once malicious cyber actors have access to a vulnerable partner, they can exploit the trust relationships between those networks.

> *In 2019, several hospitals and clinics in Australia were targeted by a ransomware incident which stemmed from a shared Managed Service Provider (MSP) that had been infected with ransomware. In order to quarantine the spread of ransomware across the networks, the hospitals isolated and disconnected a number of systems from the internet.*
>
> *As a result, access to patient records and contacts, as well as scheduling and financial management systems was significantly impacted. Medical staff had to revert to manual paper-based administration, requiring patient appointments and surgeries to be rescheduled.*

Rapid adaptation to vulnerabilities

Globally, COVID-19 themed scams occurred during the height of the pandemic last year, and could potentially increase and impact the distribution and administration of vaccines. While the ACSC has not yet observed this activity in Australia, international reporting suggests cybercriminals are attempting to scam the public in other countries by taking advantage of the COVID-19 vaccine rollout, and targeting companies involved in vaccine supply chains.

Australia continues to see cybercriminals and state-based actors rapidly exploiting vulnerabilities, with the Microsoft Exchange and Accellion File Transfer Application vulnerabilities as notable examples in 2021. According to the ACSC, malicious cyber actors were able to rapidly exploit these vulnerabilities at scale, including against targets in Australia.

The rapid exploitation of vulnerabilities by malicious actors is also changing the practices some businesses employ with third party software and services. Incidents such as SolarWinds in late 2020 have challenged the trust model that has been the norm in cyber security. The impact of this has been for some to question the practice of patching and updating systems as soon as possible after a patch has been released. This best practice norm may now be considered by some businesses to be a risk when patches could introduce new vulnerabilities that are rapidly exploited.

However, delaying applying patches and updates could itself result in compromise. A better approach to addressing this risk is for organisations to obtain assurance that their vendors implement best practice cyber security rather than simply trusting them, and for organisations to configure their network and computers to minimise the impact of running malicious software.

Building on the evolving environment, the substantial shift to remote working in the past 12 months has also introduced new opportunities for malicious cyber actors to exploit organisations and individuals online. The introduction of new devices and software to corporate networks widened the surface through which malicious cyber actors could target organisations.

Recommendations for focus over the next year

The Committee will continue to advise the Government on contemporary cyber security issues and approaches for effective implementation of the Strategy.

The dynamic nature of the digital threat environment means the implementation of the Strategy needs to be flexible to adapt to the changing landscape. Informed by recent developments within the threat environment and the progress of the Strategy to date, the Committee recommends the following areas for particular focus over the next 12 months:

- **Cyber security awareness raising.** While there is a lot of concern across the community regarding cyber threats, there is a large segment that is not aware of how, or where to find information to mitigate these risks. Evidence suggests that while Australian individuals and SMEs are improving their cyber resilience, they still remain highly vulnerable to cybercrime at a time when cybercriminals are becoming increasingly sophisticated. The Committee encourages Government to commit additional effort to raise awareness of cyber threats and mitigations with the public and SMEs. Additional funding should be considered to support mainstream and social media initiatives, enabling Government to use one voice with a clear and simple call to action, particularly around basics such as the importance of using strong passwords, patching software and maintaining current backups and ensuring these are kept offline.
- **Workplace readiness.** As we move into the future, higher degrees of hybrid and remote working are likely to be a more permanent feature. Organisations need to ensure they have the right defences in place to protect the workplace of the future. Cyber security literacy and training should be built-in to standard work practices, taking into consideration remote working in the same way that Workplace Health and Safety has now become a shared responsibility by individuals. This will mean that more people will be able to identify and raise cyber threats or incidents to the attention of responders.
- **Australian Cyber Security Centre's Joint Cyber Security Centres.** The Committee encourages Government to continue to elevate the profile of JCSCs as hubs. These offer an excellent platform to promote collaboration between Commonwealth, states and territories, and businesses that have not yet been fully leveraged. This could include further outreach events with educational institutions as well as events targeting business leaders who would not normally attend the JCSCs, such as a CEOs, and other initiatives. Timely sharing of information at scale between industry and government is also another

key role of the JCSCs and a key element of enhancing Australia's cyber resilience in an ever-evolving threat environment. The Committee recommends JCSCs play a stronger role with Government and industry on alignment of bi-directional threat sharing capabilities to enhance industry's ability to implement effective cyber protections and block threats at scale, such as through Cleaner Pipes initiatives.

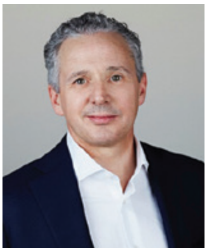
- **Australia's International Cyber and Critical Technology Engagement Strategy.** It is critical Australia continues to work closely with other international like minded nations in improving our cyber defences. This has become increasingly important due to concentration and vulnerabilities in key supply chains that underpin the digital world, such as rare metals, silicon chip sets, and telecommunications radio access technologies, including 5G. These supply chains, and others, are critical to Australia's digital economy aspirations. Technical standards also play an important role. Technical standards underpin the global marketplace and translate ethical frameworks for critical technologies into practice. The Committee encourages Government to work closely with industry bodies to determine priority areas for international standards development and make more use of private sector expertise and international networks. This could include discussing shared objectives in advance of negotiations in multi-stakeholder forums and seeking technical assessments of proposed standards by industry experts.
- **Evaluation and measuring cyber security maturity.** The Strategy, in combination with a range of other Government initiatives, seeks to uplift Australia's cyber resilience and promote a secure digital economy. Evaluating the overall maturity of Australia's cyber capabilities is a complex undertaking and challenging to communicate in a clear way to stakeholders. The Government has established an Evaluation Approach, however, the Committee encourages Government to identify and report key measures to monitor the effectiveness of the Strategy's initiatives and track our maturity over time.
- **Best Practice Regulation Taskforce.** The Government has establish the Best Practice Regulation Taskforce with a view to reviewing consumer protection, privacy and governance arrangements to determine whether they need to be clarified or uplifted to address cyber security concerns across the economy. The Committee recommends that the Government consult deeply and broadly with industry in this process with a view to mitigating regulatory burden.
- **Ransomware.** As discussed in this report, ransomware is one of the most prominent forms of malicious cyber activity today, but can be mitigated by uplifting baseline cyber security. Businesses face complex decisions when they are a victim of a ransomware attack. The Committee recommends further advocacy by Government through awareness programs on how individuals and businesses can protect themselves from ransomware attacks, the development of a clearer policy position on the payment of ransoms by organisations subject to ransomware attacks, as well as undertaking a review of cyber insurance regimes to understand their efficacy in mitigating cyber threats.
- **Cryptocurrency.** Cryptocurrency's underlying technology provides broad opportunities for innovation in a range of areas, and in some cases cryptocurrencies themselves may present meaningful opportunities in the future. However, cryptocurrency is increasingly being used by criminals in ransomware attacks affecting Australian organisations and individuals. While Australia's current anti -money laundering and counter-terrorism financing regime captures the exchange of cryptocurrency for fiat currency, it does not apply to exchanges between different types of cryptocurrencies or to transfers of cryptocurrencies between digital wallets. Increasing visibility of these transactions

would assist law enforcement in tracking the flow of cryptocurrencies associated with a ransomware attack, and should be an important area of focus for the Strategy in the coming period.

Further out

- **Uplifting quantum encryption.** An increase in the sophistication and availability of computing power will present challenges for the security of encrypted algorithms over the longer term, particularly when quantum computing becomes commercially available. If Government and industry do not concurrently uplift the encryption technology they employ, the confidentiality of data protected by current methods may be at risk. The Committee encourages Government to consider mechanisms to promote the development of quantum-resistant encryption to protect against this risk vector. These could include targeted or incentivised research and development funding, and vulnerability assessments of sensitive data holdings.

Appendix A: Cyber Security Industry Advisory Committee Members



Mr Andrew Penn

Mr Penn is Chief Executive Officer and Managing Director of Telstra, Australia's largest telecommunications company. He has had an extensive career spanning 40 years to CEO and CFO level and across three industries - telecommunications, financial services and shipping. He is a board director of the GSMA representing the telecommunications industry globally and a supporter of numerous charitable and social causes.

Ms Cathie Reid AM

Ms Reid is the Chair of AUCloud and Co-Founder of Icon Group, a provider of integrated cancer care services with operations in Australia, Singapore, New Zealand and China and served as Digital Advisor to the Icon Group board until July 2020. She is also the Managing Partner of Australia's Epic Pharmacy Group. Ms Reid was honoured with a Member of the Order of Australia (AM) in June 2019 for significant service to healthcare delivery and philanthropy, and has been recognised with numerous business awards over the course of her career.

Mr Darren Kane

Mr Kane has been the Chief Security Officer (CSO) at NBN Co since March 2015. As CSO, Mr Kane has sole accountability for enterprise-wide management of all security risks in Australia's biggest infrastructure project. His career has included 13 years with the Australian Federal Police and 6.5 years with the Australian Securities and Investments Commission. Mr Kane moved to Telstra in 2004 where he completed 11 years in varied management roles culminating in 4.5 years as Director, Corporate Security and Investigations.

Mr Chris Deeble AO CSC

Mr Deeble is Chief Executive of Northrop Grumman Australia, a provider of cyber security solutions to Australia's Defence Force. Prior to this he worked for Airservices Australia and served in the Australian Defence Force. In 2007 he was awarded the Conspicuous Service Cross. In 2016 he was appointed as an Officer of the Order of Australia for distinguished service to the Australian Defence Force.

Mr Bevan Slattery

Mr Slattery is chairman of FiberSense, a provider of continuous asset protection using virtual sensor technology over existing fibre optic networks protecting telecom, energy and other critical infrastructure assets. Mr Slattery has been heavily involved in the construction and operation of some of digital infrastructure in Australia including hyperscale data centres, international submarine cables and fibre optic networks for the past few decades and has been at the forefront of its continued expansion.

Ms Corinne Best

Ms Best leads the Trust and Risk Business at PricewaterhouseCoopers Australia (PwC) and is a member of the Executive Board. She is a Digital and Risk Professional and has been working in her field for over 22 years specialising in banking, insurance, technology and telecommunications. She is passionate about cultivating diverse and inclusive teams who are relentlessly focussed on building trust in our community and is also a supporter of charitable organisations in the Sydney area.

Mr Patrick Wright

Mr Wright is the Group Executive for Technology and Enterprise Operations at the National Australia Bank (NAB). He was appointed to the role of Chief Technology and Operations Officer in April 2017. Prior to joining NAB, Mr Wright was Global Chief Operating Officer for Barclaycard and Chief Operating Officer for Barclays Americas where he was accountable for 15,000 people. He has more than 25 years' experience in the banking and technology sectors, giving him extensive experience in driving major transformations in large financial services companies. He has moved to Melbourne from Philadelphia, US with his family to join the team at NAB. Mr Wright has a Bachelor of Business Administration, Information Systems Management from the University of Texas.

Ms Rachael Falk

Ms Falk is Chief Executive Officer of the Cyber Security Cooperative Research Centre and leads a cutting-edge program of cyber security research collaboration between government, industry and research institutions. The aim is impact, lifting Australia's cyber security capacity and capability and creating innovative solutions for the ever-evolving problems of our interconnected world. She was Telstra's first General Manager of Cyber Influence and has a background in commercial law and cyber security, practising as a lawyer at top-tier firms in Australia and the UK and in-house for Telstra. She has also worked as a cyber security consultant and is co-author of Five Knows of Cyber Security, setting an industry standard for organisational cyber security best-practice.

Professor Stephen Smith

Professor Smith is Chair of the Advisory Board, University of Western Australia Public Policy Institute and Chair of the UWA Defence and Security Institute. He is currently the Chairman of Sapien Cyber, Chair of the Strategic Advisory Group for archTIS and a member of the Board of the Perth USAsia Centre and a Member of the Board of AROSE. Professor Smith was Federal Member for Perth for the Australian Labor Party from March 1993 until September 2013. In a distinguished career spanning 20 years in the Australian Federal Parliament, Professor Smith served as the Minister for Defence, and prior to that, as

Minister for Foreign Affairs and Minister for Trade. Following his retirement from the Australian Parliament in 2013, Professor Smith became a member of the EY (Ernst and Young) Oceania Government and Public Sector Advisory Board, Chair of the Asia Desk and a member of the Advisory Board of Perth Law firm Lavan, and a member of the Board of Hockey Australia.

Mr David Tudehope

Mr Tudehope is Chief Executive and co-founder of Macquarie Telecom Group. He is responsible for overseeing the general management and strategic direction of the Group and is actively involved in the Group's participation in regulatory issues. He is a member of the Australian School of Business Advisory Council at the University of NSW and was a member of the Australian Government's B20 Leadership Group. Mr Tudehope holds a Bachelor of Commerce degree at the University of NSW and Harvard Business School's Advanced Management Program 173. In 2011, the Australian Telecommunication Users Group awarded David the Charles Todd Medal for leadership in the telecom industry. In 2018 at the 12th Annual ACOMM telecom industry awards, David received the highest award, Australian Communications Ambassador.

Appendix B:
Cyber Security Strategy 2020 Implementation Progress

Initiative	Description	Funding	Measuring Success	Implementation progress
Actions by governments				
1. 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.	**Allocated:** $8.3 million.	– 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.	– The Minister for Home Affairs introduced the Security Legislation Amendment (Critical Infrastructure) Bill 2020 into Parliament in December 2020. – The Bill is currently being considered by the Parliamentary Joint Committee on Intelligence and Security. The first hearing was held on 11 June 2021, and a second was on 8–9 July 2021. – Industry co-design of sector specific requirements commenced in early 2021.

Initiative	Description	Funding	Measuring Success	Implementation progress
2. Enhance incident response procedures	The Australian Government will invest in 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.	**National Exercise Program** **Allocated:** $10.0 million.	– Updated Cyber Incident Management Arrangements (CIMA) 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.	– ACSC leads regular national exercises with Commonwealth, state and territory agencies, and industry. – ACSC has undertaken offensive cyber effects to dismantle cybercrime operations. – In December 2020, Government with states and territories developed a survey to review the CIMA through the National Cyber Security Committee (NCSC). – NCSC Policy Subcommittee has developed a report on the CIMA review including recommendations to update the CIMA in 2021.

Initiative	Description	Funding	Measuring Success	Implementation progress
3. Bolster law enforcement capabilities, including on the dark web	The Australian Government will strengthen law enforcement's counter cybercrime capabilities. This includes an investment in the AFP to set up target development teams and bolster its ability to go after cybercriminals. 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 cybercriminals. The Australian Government will ensure it has fit-for-purpose powers and capabilities to discover, target, investigate and disrupt cybercrime, including on the dark web. The Australian Government will extend and expand the ACSC's ability to counter cybercrime actors offshore and provide technical advice and assistance to Commonwealth, state and territory law enforcement agencies in identifying and disrupting cybercriminals. This builds on the Australian Government's election commitment to counter foreign cybercriminals. Combined, these initiatives will enable government to take the fight to foreign actors that seek to target Australians.	**AFP activities** **Allocated:** $89.9m. **Countering cybercrime offshore** **Allocated:** $31.6 million.	– Through enhanced capabilities and coordination, the AFP, ACIC and the ACSC identify and disrupt more cybercrime targets. – Agencies have the authorities they need to discover, target, investigate and disrupt cybercrime and cyber-enabled crime. – More responses to online crimes are coordinated between the Australian Government, states and territories.	– The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 was introduced to Parliament in December 2020. The Bill is currently being considered by the Parliamentary Joint Committee on Intelligence and Security. – A new National Plan to Combat Cybercrime is under development for delivery in the second half of 2021. Consultation with industry stakeholders commenced in May 2021. – The AFP is continuing with their expansion of multi-disciplinary cybercrime investigation teams across Australia, comprised of investigators, intelligence analysts and technical specialists. – The AFP continues to integrate into the ACSC. – ASD has assisted to remove over 6000 websites hosting cybercrime activity from the internet. – ACSC has supported law enforcement partners, and used its offensive cyber capabilities to generate effects to undermine and disrupt cybercriminals offshore.

Initiative	Description	Funding	Measuring Success	Implementation progress
4. 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.	**Allocated:** $18.8 million with additional costs to be absorbed by agencies implementing the Cyber Hub pilot program.	– Centralisation of Australian Government IT networks makes it easier to defend against malicious activity.	– A 12 month pilot commencing mid-2021 is being undertaken, to demonstrate the Cyber Hub concept.
5. Improve threat information sharing	The Australian Government will, through the ACSC, deliver a new partner portal coupled with a multi-directional threat-sharing platform. The Australian Government will enhance the cyber security of Australian universities through a threat intelligence-sharing network, sector-wide threat modelling and a national cyber security forum that will meet three times a year.	**Threat-sharing platform** **Allocated:** $35.3 million. **Cyber Security of universities** **Allocated:** $1.6 million.	– Government and businesses and the Australian University sector have increased visibility of cyber threats in near real-time. – There is increased two-way flow of cyber security information.	– ASD has undertaken a range of threat briefings to share information at JCSCs. – ACSC has also commenced co-design with industry for the establishment of its cyber threat intelligence sharing (CTIS) platform. – RMIT is supporting the development of threat modelling activities for the university sector.

Initiative	Description	Funding	Measuring Success	Implementation progress
6. Uphold existing international law and norms of responsible 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.	**Allocated:** Nil. This project is to be delivered through existing funding.	– 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.	– In April 2021, the International Cyber and Critical Technology Engagement Strategy was released.
7. Strengthen cyber security partnerships	The Australian Government will expand the ACSC's JCSC program. A broader range of ACSC staff and capabilities will be available to enhance collaboration with and support state, territory and local governments, industry partners and academia across the country. The Australian Government will also establish a Department of Home Affairs presence at each JCSC to provide a whole-of-government approach to cyber security engagement.	**JCSC Program expansion** **Allocated:** $67.9 million. **Home Affairs JCSC outreach officers** **Allocated:** $8.2 million.	– Customer experience survey data indicates effective partnerships between businesses and government.	– ACSC has hosted over 200 events at JCSCs, including threat briefings for specific sectors. – ACSC has opened a JCSC outreach office in Darwin in cooperation with the Northern Territory Government. – ACSC has supported cyber security preparedness exercises to be run from the JCSCs. – ACSC has expanded the ACSC Partnership Program, with Network Partners growing by over 130% between June 2020 and June 2021. – Recruitment of Home Affairs outreach officers is underway. Five positions have been filled by mid-2021. The remaining positions will be filled in 2021-22.

Initiative	Description	Funding	Measuring Success	Implementation progress
8. 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.	**Allocated:** Nil. This project is to be delivered through existing funding.	– Consultation is undertaken on possible future reforms to clarify cyber security obligations for Australian businesses.	– Public consultation on cyber security reforms is expected to begin in mid-2021.
9. Stay ahead of the technology curve	The Australian Government will expand its data science capabilities, ensuring Australia remains at the forefront of the technological advancements in cyber security. The Australian Government will also establish cutting-edge research laboratories to better understand threats to emerging technology. Five hundred additional intelligence and cyber security personnel will be recruited over the next 10 years. The Australian Government will enable and enhance cyber security intelligence capabilities.	**Data capabilities** **Allocated:** $118.0 million. **Research laboratories** **Allocated:** $20.2 million. **500 cyber security personnel** **Allocated:** $469.7 million. **Enhance intelligence capabilities** **Allocated:** $385.4 million.	– The Australian Government has sovereign research capability to assess vulnerabilities in emerging technology.	– Planning and implementation underway.

Initiative	Description	Funding	Measuring Success	Implementation progress
Actions by businesses				
10. 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 funding 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 deliver a national situational awareness capability to better enable the ACSC to understand and respond to cyber threats on a national scale.	**Vulnerably assessments Allocated:** $66.5 million. **National situational awareness capability Allocated:** $62.3 million.	– 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.	– The Minister for Home Affairs introduced the Security Legislation Amendment (Critical Infrastructure) Bill 2020 into Parliament in December 2020. Key features of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 include Enhanced Cyber Security Obligations, and Government Assistance to relevant entities for critical infrastructure assets in response to cyber-attacks. – The Bill is currently being considered by the Parliamentary Joint Committee on Intelligence and Security. The first hearing was on 11 June 2021, and a second was held on 8–9 July 2021. – Industry co-design of sector specific requirements commenced in early 2021. – Government has commenced engagement with critical infrastructure providers to voluntarily assess cyber security capability maturity and recommend mitigations. An open-source intelligence collection capability was developed to inform the national situational awareness picture. – ACSC has also made enhancements to ReportCyber to facilitate improved incident reporting and development of a national threat picture.

Initiative	Description	Funding	Measuring Success	Implementation progress
11. Uplift the cyber security of SMEs	The Australian Government will establish the Cyber Security Connect and Protect Program to equip trusted organisations like chambers of commerce and business associations to raise the cyber security of SMEs in their local area.	**Allocated:** $8.3 million.	– An increasing number of small businesses are improving their cyber security practices.	– Cyber Security Connect and Protect Program launched October 2020. 14 successful applicants were announced in April 2021. Projects to be completed by March 2022, program evaluation to commence in 2022-23.
12. 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. The Australian Government will provide consumers with information about what to take into consideration when purchasing Internet of Things devices. In the longer term the Government will consider whether additional steps are needed to inform consumers, such as cyber security product labelling.	**Allocated:** $2.1 million.	– Businesses have a better understanding of best practice security controls for the Internet of Things.	– The Minister for Home Affairs released the Voluntary Code of Practice: Securing the Internet of Things in September 2020. – The Government is considering whether additional action on Internet of Things security is needed, with public consultation expected to begin in mid-2021.

Initiative	Description	Funding	Measuring Success	Implementation progress
13. Grow a skilled workforce	The 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 Cyber Security Skills Partnership Innovation Fund will create new opportunities for industry and education providers to partner on innovative skills projects that increase the quality and quantity of cyber security professionals. The ACSC will grow its education, skills, training, mentoring and coaching programs, including specialised programs for women. The Australian Government will equip Questacon to design challenges and teacher training that prepare primary, secondary and tertiary students for a career in cyber security for Cyber Ready and Engineering is Elementary programs. The Australian Government will enhance data collection on the cyber security skills shortage. The Cyber Security National Workforce Growth Program complements the 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.	**Cyber Security Skills Partnership Innovation Fund** **Allocated:** $70.3 million. **ACSC skills programs** **Allocated:** $6.3 million. **Questacon Programs** **Allocated:** $14.9 million. **Data Collection** **Allocated:** $2.5 million **Australian Defence Force (ADF) Cyber Gap Program** **Allocated:** $41.1 million.	– 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.	– Round 1 of the Cyber Security Skills Partnership Innovation Fund was announced on 4 February 2021 and applications closed 11 March 2021. Successful applicants were announced on 29 June 2021. – The ACSC launched the pilot of the Australian Women in Security Network Mentoring program in May 2021. – Questacon pilots, workshops and focus groups continue to be delivered ahead of broader classroom and teacher roll-out. Over 850 teachers have participated in Engineering is Elementary workshops across Australia. – Targeted Update of ANZSCO for inclusion of cyber security occupations as part of enhanced data collection is underway and due for release in November 2021. – ADF Cyber Gap Year Pilot Program commenced in July 2020 with 47 participants, with 46 graduated in June 2021. 271 participants are undertaking the 2021 intake. – Government is considering options to strengthen Voluntary Professional Accreditation of Tertiary Cyber Security Courses in relation to workforce professionalisation.

Initiative	Description	Funding	Measuring Success	Implementation progress
14. 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 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.	**Allocated:** Nil. This project is to be delivered through existing funding.	– More known malicious threats are prevented from reaching Australians.	– Preliminary discussions between Government and businesses are underway to consider how it can better support industry implement threat blocking technology. – ASD has piloted a Protected Domain Name Server service on government systems, which blocks known 'bad' domains or malicious actors. – ASD has deployed over 36,000 host-based sensors to Government agencies to monitor for threats.

Initiative	Description	Funding	Measuring Success	Implementation progress
Actions by the community				
15. Access guidance and information on cyber security	The community should 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 conduct 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 Australian Government's investment to boost eSafety's investigations and support teams so help is available to Australians when they encounter harmful content and behaviours online.	**Cyber Security Awareness Raising campaign** **Allocated:** $4.9 million.	– 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.	– ASD commenced a new cyber security awareness campaign, providing targeted advice to small businesses and individuals, in November 2020. – The cyber security awareness raising campaign development is underway, leveraging ASD's new campaign and including due diligence in accordance with guidelines for Government advertising campaigns.

Initiative	Description	Funding	Measuring Success	Implementation progress
16. 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 cybercrime. The Australian Government will enhance customer engagement channels and 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 investment in support of the ACSC expanding its assistance to the SMEs and the community. The Australian Government will also bolster services to victims of identity and cybercrime.	**Enhance customer engagement channels** **Allocated:** $58.3 million. **24/7 Helpdesk** **Allocated:** $12.3 million. **Bolster services to victims of identity and cybercrime** **Allocated:** $6.1 million.	– Increased availability and quality of support services for victims of cybercrime. – Increased availability of cyber security advice and assistance for all Australians, including through the ACSC's expanded 24/7 helpdesk. – Increased understanding of the impacts of cybercrime on the community.	– IDCARE was allocated funding to bolster services to victims of identity and cybercrime in early 2021.

Initiative	Description	Funding	Measuring Success	Implementation progress
17. 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.	**Allocated:** $2.1 million (allocated under *'Create a more secure Internet of Things'*).	– Community awareness of how to purchase secure digital products and services.	– The Government is considering whether additional action is needed to inform consumers about the cyber security of technology products, such as cyber security labelling. Public consultation is expected to begin in mid-2021.
Other commitments				
18. Update the National Identity Security Strategy	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 cybercrime.	**Allocated:** $2.8 million to be absorbed from within the Department of Home Affairs' budget.		– The 2021-22 Budget included an investment of $2.8 million, in support of the Digital Economy Strategy, to strengthen Australia's national system of identity settings. – The Government has worked throughout 2020-21 with stakeholders to develop proposals to strengthen national identity arrangements.
19. Supply Chain Principles	The Australian Government will co-design supply chain principles for decision makers and suppliers to encourage security-by-design, transparency and integrity in procurement.	**Allocated:** Nil. This project is to be delivered through existing funding.		– A Critical Technology Supply Chain Principles paper was released on 22 October 2020, and submissions closed 20 November 2020. The principles are under development and to be released by end of 2021.

Appendix C - Overview of Australian Government initiatives on cyber security

Protecting Australians and enabling the secure foundations of Australia's Digital Economy Strategy to build a modern and resilient economy to drive Australia's future prosperity

Securing Government

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, and will increase opportunities to focus the Australian Government's cyber security investment.

Raising Awareness & Protecting Consumers

In order to combat cybercrime and strengthen the cyber resilience of our communities, there needs to be a continued effort to raise cyber awareness for all Australians. The Committee has provided advice to Government on raisin g the public's cyber security awareness, including through the national cyber security awareness raising campaign. The $4.9 million awareness raising initiative outlined in the Strategy is currently under development. The Australian Government will invest $12.3 million to extend a 24/7 cyber security helpdesk to SMEs and families, in addition to $6.1 million to support victims of identity and cybercrime across our communities.

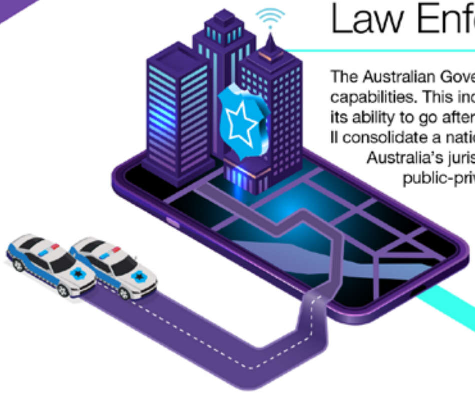
Skills

Since the launch of Australia's Cyber Security Strategy 2020, the $50.0 million Cyber Security National Workforce Growth Program has been expanded by a further $43.8 million. The 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.

The Skills Partnership Innovation Fund will create new opportunities for businesses and academia to partner on innovative skills projects that directly meet employers' skills needs ($70.3 million). $2.5 million will be allocated to enhanced data collection on the cyber security skills shortage. The ACSC will grow its education, skills, training, mentoring and coaching programs, including specialised programs for women ($6.3 million). Questacon will design challenges and teacher training that prepare primary, secondary and tertiary students for a career in cyber security ($14.9 million). The Cyber Security National Workforce Growth Program complements the $40.0 million invested by the Australian Government 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.

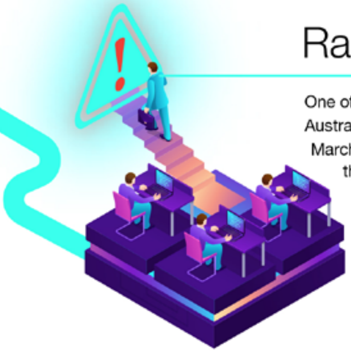
Small to medium Enterprise (SME)

The $8.3 million Cyber Security Connect and Protect Program will equip trusted organisations such as chambers of commerce and business associations to raise the cyber security of SMEs in their local area.



Law Enforcement

The Australian Government will invest $124.9 million to strengthen law enforcement's counter cybercrime 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 cybercriminals. A new National Plan to Combat Cybercrime is currently being developed and wi ll consolidate a national framework to bring together the powers, capabilities, experience and intelligence of all of Australia's jurisdictions to build a strong operational response to cybercrime, while focussing on strengthening public-private partnerships, and providing better support to the victims of cybercrime.



Ransomware

One of the most prominent cybercrimes facing Australian business today is ransomware. In March 2021, the Committee's first public thought-piece was published on the topic of ransomware, urging Australians and their businesses, no matter how big or small, to strengthen their cyber defences and protect themselves from this increasingly complex and impactful cyber threat.

Critical Infrastructure

After an extensive co-design process with industry, the Security Legislation Amendment (Critical Infrastructure) Bill 2020 is being considered by Parliament and work has commenced to develop sector-specific rules to underpin the legislation. This will serve to strengthen the resilience of critical services and systems that all Australians rely on to live and work.

Cyber security, safety and trust

Cyber security, safety and trust are the keystone of our digital economy. Government investments in safety and security are enabling businesses to actively engage in the digital economy with confidence.

New investments under the Digital Economy Strategy include:

- Additional funding for the Cyber Security Skills Innovation Partnership Fund to a total of $70.3m (an initiative under Australia's Cyber Security Strategy 2020)
- Securing 5G and future 6G connectivity
- Ensuring the security of Australian Government data
- Underpinning the digital environment with trusted identity
- Digital Skills Cadetship Trials
- Next Generation Technology Graduates Program (please note this program is focused on emerging technologies, of which cyber security is one possible area).

Improve Threat Information Sharing and Industry Collaboration

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 committed $67.9 million to expand the Joint Cyber Security Centre (JCSC) program to broaden capabilities of the JCSCs and drive enhanced collaboration across state, territory and local governments, as well as industry and academia. An additional $1.6 million will enhance the cyber security of universities by funding a threat intelligence-sharing network, sector-wide threat modelling and a national cyber security forum that will meet three times a year.

Smart Manufacturing

The $1.5 billion Modern Manufacturing Strategy is designed to ensure Australian manufacturers scale-up, become more competitive and more resilient. There is tremendous potential for innovation and growth through smart manufacturing, however, this brings new risks and challenges including cyber security.

With the interconnectedness of smart factory technologies, cyber threats are among the most prevalent, as smart factory environments expose people, technology, physical processes, and intellectual property to cyber vulnerability.