Australia's Cyber Security Strategy 2020

Cyber Security Industry Advisory Committee Annual Report 2022

Contact us

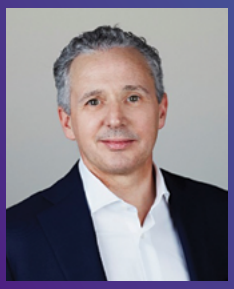
Enquiries regarding the licence and any use of this document are welcome at:

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 2022

Table of Contents



Chair's Foreword

We are living in a time of exciting and rapid technological innovation. Connected digital technologies are driving transformative change. Economic and social paradigms are shifting, markets are being reshaped. There is great promise for a more connected, more prosperous future.

But the real promise of the Digital Economy is not guaranteed. While our lives are increasingly lived online, more abundant and increasingly sophisticated cyber criminals and ever-more emboldened state actors mean Australia is now literally under constant cyberattack. In our increasingly interconnected and inter-dependent society, no one is truly safe, and no one can afford to drop their guard. The integrity and security of our digital infrastructure and platforms has never been more important.

Tackling this critical challenge is a whole of nation endeavour. It requires a clear strategy, determined action, and constant vigilance. Australia's cyber defences need to be strong, adaptive and built around a framework that is coordinated and integrated – and Australia's Cyber Security Strategy 2020 was designed to provide that framework. Development of the Strategy was shaped by advice from an expert Industry Advisory Panel.

The secret to the success of the Strategy, however, is in its implementation and that is where the Industry Advisory Committee (IAC) (the Committee) plays a key role. The Committee advises the Government on implementation from an industry perspective, helping ensure the essence of co-design remains an enduring principle.

This is the second annual report by the Committee. It provides an overview of the progress in the implementation of the Strategy by Government and developments in the threat environment. Importantly, it highlights where progress needs to be accelerated and improved in order to respond to new and emerging threats and vulnerabilities.

We hope this report builds public awareness of the importance of the Strategy, the role the Committee plays within the Australian cyber security eco-system and draws attention to the tools and information available to government agencies, organisations, and the public to help navigate an increasingly complex and dynamic cyber threat landscape.

Robust and effective cyber security is critical for our economic prosperity, international competitiveness, and national security.

However, not only is our digital infrastructure and platforms at risk from cyber-attack, but it is also exposed to other risks. These include access to critical technologies such as 5G telecommunications and semiconductors as well as maintaining interoperability of technology by increasing our role in global discussions on standards setting. This will also require us to substantially lift our digital and cyber skills.

We therefore applaud the Cyber Security Minister's decision to shape a broader National Cyber Strategy through this lens; a step which will be critical to building and protecting Australia's sovereign capability.

As Australia continues to navigate an increasingly complex cyber threat landscape, now is the appropriate time to refresh and expand from the 2020 Australian Cyber Security Strategy and the Committee looks forward to continuing to work to work with government to support effective, resilient, and agile cyber security outcomes for Australian communities and businesses.

The risks are great, the stakes are high and so many of Australia's future opportunities depend on a safe and secure digital world.

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

Introduction

This annual report from the Cyber Security Industry Advisory Committee (the Committee) addresses the following:

- progress on the implementation of Australia's Cyber Security Strategy 2020 (the Strategy)
- the Committee's work and how this translates to advice in shaping the implementation of the Strategy
- the evolving cyber threat landscape in the context of the broader digital environment
- an assessment of the effectiveness of the initiatives pursued to date
- the Committee's views on where progress needs to be accelerated and improved, as well as emerging cyber security policy issues and priorities.

Whole-of-Nation Cyber Security

Over the past two years Australia has faced a cyber landscape characterised by rapid change. Australians rely on connected services and activities more than ever, with technological innovation presenting both opportunities and challenges for Australian businesses and the economy. The global cyber threat environment has intensified, and Australia is an increasingly attractive target for malicious actors and cybercriminals.

Protecting Australia and Australians from cyber threats, while also ensuring a baseline level of cyber resilience across the economy is a key priority for the Government. To achieve this, the Government will need to take a whole of nation approach to uplifting Australia's resilience and capabilities.

The appointment of Australia's first Minister for Cyber Security to Cabinet reflects the Government's strong focus on cyber security as a national priority. It provides an opportunity to enhance coordination across government on cyber policy, strategy and response mechanisms.

Priorities for Government into the future will continue to build and expand upon the work commenced over the past two years under the Strategy.

The Strategy was released on 6 August 2020, and is supported by a $1.67 billion investment over ten years to create a more secure online world for Australians, businesses and essential services. The Strategy follows the $230 million 2016 Cyber Security Strategy, which set out a four-year plan to make Australia more resilient, boost innovation and research alongside improved skills pathways, and increasing awareness and education.

The 2020 Strategy is delivering a number of initiatives, including:

- establishing cyber security minimum standards and new information sharing obligations for critical infrastructure providers
- enhanced incident response procedures across governments and industry
- a Cyber Enhanced Situational Awareness Response (CESAR) Package to support the Australian Signals Directorate's (ASD) operational and cyber capabilities
- increasing capabilities to counter cybercrime within the Australian Federal Police (AFP)
- boosting cyber resilience and awareness campaigns targeted at the Australian public
- providing expanded resources, advice and guidance materials to small and medium enterprises (SMEs) via cyber.gov.au
- hardening Australian Government IT systems.

In addition to programs conducted under the umbrella of the Strategy, complementary work is underway to uplift cyber skills, international engagement and technical capabilities via other streams of work across government, including:

- a $37.7 million investment in growing Australia's cyber security workforce via the Modern Manufacturing Strategy
- furthering Australia's vision for a safe, secure and prosperous cyber-enabled world via the 2021 International Cyber and Critical Technology Engagement Strategy, including $20.5 million to improve cyber resilience in Southeast Asia and $17.0 million to support Australia's neighbours in the Pacific to strengthen their cyber capabilities and resilience
- building Australia's digital economy and capability in emerging technologies through the $1.2 billion Digital Economy Strategy, including investing $43.8 million in the Cyber Security Skills Partnership Innovation Fund
- the release of the Ransomware Action Plan in October 2021, highlighting Australia's capabilities to combat ransomware
- enhancing offensive and defensive cyber capabilities through the Resilience, Effects, Defence, Space, Intelligence, Cyber and Enablers (REDSPICE)– a $9.9 billion investment over 10 years that will be delivered by ASD.

The REDSPICE program is in response to the deteriorating strategic environment which in our region - the Indo-Pacific - is far more complex and far less predictable than at any time since the Second World War. Throughout recent years Australia has been targeted by a range of actors conducting cyber operations that pose a significant threat to our security. REDSPICE will grow our defensive cyber capabilities to enable hardening and defence of our national systems and critical infrastructure. It will also enhance the intelligence capabilities of the ASD to support our cyber defence. REDSPICE incorporates some initiatives that were previously in the CESAR program, moving them forward in time for delivery and expanding them. As part of this investment ASD will have significantly larger footprints in Melbourne, Brisbane and Perth thus eclipsing the smaller ASD-JCSCs currently in those cities. In terms of initiatives directly relevant to cyber defence REDSPICE will deliver the following:

- Improve resilience of critical infrastructure against sophisticated cyber attacks
- Increase the visibility of threats to Australia's most critical systems
- Improve machine time cyber threat intelligence sharing across government and industry
- Double persistent cyber hunt activities and nationwide cyber incident response
- Increasing understanding of adversaries capabilities, intent, and decision-making
- Double ASD's analytical workforce.

Completed initiatives under the Strategy

In the 2021-22 financial year, a range of important framework documents, legal instruments and new initiatives were finalised and implemented, including:

- on 21 March 2022, the National Plan to Combat Cybercrime was publicly released, providing a unifying vision to support ongoing and evolving action to combat cybercrime
- on 8 December 2021, the *Autonomous Sanctions Amendment (Magnitsky-Style and Other Thematic Sanctions) Act 2021* commenced. The Act modernises Australia's autonomous sanctions framework, enabling the Foreign Minister to sanction individuals or entities involved in actual or attempted significant cyber incidents
- on 25 November 2021, the *Telecommunications (Interception and Access) Amendment (2021 Measures No. 1) Regulations 2021* came into effect, clarifying that telecommunication providers can deploy threat blocking technology to identity and block malicious SMS scams at scale on their own networks
- on 15 November 2021, the Critical Technology Supply Chain Principles (the Principles) were released. The Principles provide guidance to governments and business in making decisions about their critical technology suppliers, and the transparency of their products. The Blueprint and Action Plan for Critical Technologies was released on 17 November 2021, complementing the Principles
- on 31 October 2021, the public awareness campaign 'Beat cybercrime in your downtime' launched to encourage Australians to rethink their perspective on cyber security and to take easy steps to become more cyber secure.

The Industry Advisory Committee

The establishment of the Industry Advisory Committee was announced on 20 October 2020 to provide independent strategic advice on Australia's cyber security challenges and help guide the Strategy's implementation from an industry perspective.

The Committee comprises industry experts from diverse disciplines as listed below. Additional details on the Committee members are included in **Appendix A**.

- Andrew Penn, Industry Advisory Committee Chair, Chief Executive Officer of Telstra
- Cathie Reid AM, Industry Advisory Committee Deputy Chair, Chair of AUCloud
- Darren Kane, Chief Security Officer of NBN Co
- Chris Deeble AO CSC, Chief Executive of Northrop Grumman Australia
- 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.

As Australia continues to navigate an increasingly complex cyber threat landscape, the Committee will continue to work with government and will advise and advocate for effective, resilient and agile cyber security outcomes for Australian communities and businesses.

Recommendations for Immediate Focus

Much has been achieved since the Strategy was launched in 2020 as outlined in this report and the Committee's 2021 Annual Report. However, notwithstanding the many initiatives launched by Government, there are areas where progress has either been insufficient or needs to be accelerated and improved to respond to the changing landscape.

More information on the Committee's work, including recommendations made in two thought-pieces published throughout the year is provided on **pages 25 to 27**. However, the most urgent and important issues and priorities in the minds of the Committee are listed below.

Hardening Australian Government IT Systems

One of the key aims of the Strategy is for government to substantially lift the level of cyber security resilience across its own operations. Government systems continue to be a prime target for malicious actors. There have been many examples of attacks on infrastructure both at a state and federal level, including service delivery agencies, government departments and political offices.

The Cyber Hubs that have been established to lead this, coordinated by the government's Digital Transformation Agency, need to be given more teeth and their work needs to be accelerated.

So far under the Strategy, the Government has been significantly focussed on what business needs to do to improve its cyber defences. It is also important that government makes progress to harden its own systems and cyber defences. In asking Australians and Australian businesses to support the Strategy, government needs to be role-modelling cyber best practice in its own operations, while also improving the security of increasingly digital government service delivery.

Governance and Measurement

Developing an empirical, data-driven measurement system of Australia's cyber security maturity has been a key and consistent recommendation of the Committee since its inception. Although the initiatives under the Strategy are having a positive impact, the threat landscape continues to evolve and the level and sophistication of malicious cyber activity is increasing.

Without a rigorous evaluation and measurement system and against an evolving maturing index, there is too much reliance on qualitative anecdotes and commentary to determine the progress and effectiveness of initiatives under the Strategy. The Strategy is critical to the security of Australia, and Australia should be able to point to data and quantifiable proof points to maintain confidence in its progress in uplifting cyber resilience.

The overall implementation of the many initiatives in the Strategy would also benefit from a stronger integrated governance approach with stronger line of sight to implementation progress.

Protecting Critical Infrastructure and Systems of National Significance (CI-SONS) industry engagement

It is important to maintain meaningful engagement and consultation in the development of industry regulations for the CI-SONS legislation. This legislation is a cornerstone of the Strategy, and ongoing industry consultation will be crucial to the legislation being embraced successfully by businesses.

For most of the 11 sectors identified as critical infrastructure under the legislation, the obligations are new. The supporting regulations and any future amendments will need to be carefully designed and implemented in partnership and consultation with businesses to reflect the specific dynamics, technology and characteristics of each sector, ensuring a baseline uplift across all sectors.

Awareness raising

The volume of malicious cyber activity is increasing significantly and many of the programs under the Strategy are aimed at hardening Australia's systems and defences against this. While these programs include identifying and blocking malicious traffic before it reaches the public, Australia will never be able to stop all malicious activities. Therefore, individual awareness and good cyber defence hygiene is essential.

It is often the human element that leads to cyberattacks being successful. Increasing cyber awareness within the community is therefore one of the most important priorities. This is about getting the basics right.

There have been a number of cyber awareness campaigns and initiatives launched under the Strategy, and their results are positive. However, the resources and investments being committed to them is far too low when considered in the context of the total investment in the Strategy, the scale of the challenge, and the extent to which increasing awareness can make a difference.

Threat sharing

Threat sharing and collaboration are crucial to improving Australia's defences. The government's Cyber Threat Information Sharing Platform (CTIS) will help address long-standing industry requests for improved threat indicator sharing. The priority is now the onboarding process for the many organisations interested in joining the platform in a timely and streamlined manner, and dedicating resources to ensuring continuous quality assurance of inputs.

Another important initiative under the 2016 Cyber Security Strategy was the establishment of the Joint Cyber Security Centres (JCSCs) under the ASD's Australian Cyber Security Centre (ACSC). These are the key vehicles to increase collaboration between government and industry at the federal and state and territory levels.

The progress in establishing and maturing the JCSCs has been too protracted to date and should be accelerated by providing collaboration opportunities between the ASD and industry subject matter experts based in capital cities where JCSCs are located.

Ensuring that industry cyber leaders remain key partners in the governance and directional focus of the JCSCs will also assist government to remain focussed on the most pressing issues facing the nation.

Best Practice Regulation Taskforce (the Taskforce)

The purpose of the Taskforce's work in 2021 was to consider, in consultation with industry and other key stakeholders, what changes or clarifications may be required to existing legislation to address cyber security issues.

The work is aimed at businesses not captured under the CI-SONS reforms. The Taskforce explored whether existing legislation, such as corporate, consumer and privacy laws, sufficiently captures responsibilities and accountabilities in relation to cyber security.

In July 2021, the Taskforce consulted with industry over a seven-week period. Given the time that has passed since this consultation period, Government should prioritise providing industry with feedback on the conclusions from this work, including gaps in current legislation and any proposed initiatives or changes being considered.

It has been the Committee's view that any interventions should minimise legislative change and focus on voluntary industry standards.

This is an important body of work which is crucial to further protect consumers.

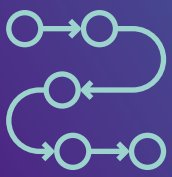
Cyber security skills

If we are to meet all of these challenges and thrive in the accelerating digital world, we are going to need to substantially uplift our cyber skills base. And we are going to need to do this right the way across the spectrum from deep cyber expertise to basic cyber hygiene practices. Through our schools and universities, governments and industry; and we are going to need to it fast.

Access to Critical Technologies and Global Technology Standards

While the Strategy, and therefore the role of the Committee, is focused on strengthening our cyber defences, there are other threats to the digital infrastructure that supports our digital lives. In particular, long term supply chains of critical technologies, for example, 5G radio access technologies and semiconductors, as well as global standards that ensure technology interoperability.

What is clear therefore is as our world becomes more digitally enabled, a more holistic and integrated approach to ensuring the integrity of our digital infrastructure is becoming increasingly important. We discuss this dynamic further in this report, and encourage the Government to shape its digital policies, including the Cyber Security Strategy, through this lens.



The Strategy's implementation progress

This section provides a summary of the progress of key initiatives under the Strategy.

A more detailed account of the Strategy's progress can be found in **Appendix B**.

Governance and evaluation mechanisms

At the Strategy's launch, the following governance bodies were established to provide oversight and manage risks raised throughout the Strategy's implementation:

- the Industry Advisory Committee
- the Interdepartmental Committee on Cyber Security
- a Commonwealth Deputy Secretary level committee focussed on strategic coordination across government
- the Cyber Security Strategy Delivery Board (a Commonwealth senior executive board focussed on inter agency coordination and implementation of programs).

Program-level evaluations continue to measure the impact and effectiveness of the Strategy's initiatives on a business as usual basis.

The government has advised the Committee that a strategic evaluation framework is being progressed in 2022 and will provide an assessment of the progress, impact and value of the Strategy.

The Committee has advised that it is crucial for the success of the Strategy that the evaluation framework needs to be accelerated and underpinned with a strong empirically based measurement framework to monitor and gauge the implementation and effectiveness of the initiatives under the Strategy, including consideration of an overall maturity index.

Critical Infrastructure and Systems of National Significance (CI-SONS)

The Government has developed reform initiatives to uplift the security and resilience of Australia's critical infrastructure, including broadening the Trusted Information Sharing Network (TISN) and supporting legislative reforms.

This package is complemented by the ASD's work to assist Australia's major critical infrastructure providers to assess their networks for vulnerabilities and to enhance their cyber security posture.

Legislative reforms

In consultation with industry, the former Government progressed reforms for CI SONS. 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.

Amendments to the Security of Critical Infrastructure Act 2018 (SOCI Act) have strengthened Australia's ability to manage and respond to security risks to critical infrastructure. The *Security Legislation Amendment (Critical Infrastructure) Act 2021* came into force on 2 December 2021. The second tranche of reforms came into effect on 2 April 2022, under the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*.

Amendments to the SOCI Act have:

- expanded the definition of critical infrastructure to cover 11 sectors and 22 asset classes
- introduced a cyber incident reporting regime for critical infrastructure assets and a risk management program obligation (which, along with the pre-existing Asset Registration obligation, may apply to all 22 asset classes)
- enabled government assistance in response to industry cyber incidents in defined circumstances.

Amendments also introduced the ability for the most important and interdependent critical infrastructure assets to be declared Systems of National Significance, which may be subject to enhanced cyber security obligations.

The obligations which may apply to a System of National Significance will vary, and should an obligation apply, it will depend on the specific role and function of that asset. This recognises that different sectors have different networks and systems, and face different risks. Enhanced cyber security obligations may include:

- developing cyber security incident response plans to prepare for a cyber security incident
- undertaking cyber security exercises to build cyber preparedness
- undertaking vulnerability assessments to identify areas for remediation
- providing system information to government to facilitate an increased threat picture.

The Committee continues to encourage government to engage and consult with operators of critical infrastructure through the development of sector-specific regulations. Some sectors, such as telecommunications and financial services, are experienced with the obligations under the amendments to the SOCI Act as they have operated under similar sectoral regimes for many years. However, for the majority of the sectors identified as critical infrastructure, these are new obligations and it will take time and support for the operators in those sectors to adapt to them.

Trusted Information Security Network (TISN)

The TISN is a partnership forum, comprising industry and all levels of government, where members can engage on approaches to enhancing the security and resilience of critical infrastructure in the face of all hazards. Government is expanding the TISN membership be more reflective of Australia's critical infrastructure sectors, and to share updates to a broader section of the critical infrastructure community on threats, including cyber security threats.

From the Committee's perspective, threat sharing is the key to threat blocking which is in turn, the key to cleaner pipes.

The Critical Infrastructure Uplift Program (CI UP) Pilot

The ASD voluntary CI-UP assists critical infrastructure providers to evaluate the cyber security maturity of their CI-SONS, deliver prioritised vulnerability and risk mitigation strategies, and to implement the recommended risk mitigation strategies. More than 100 CI providers had registered interest by the end of June 2022.

In the 2021-22 financial year, the ASD completed two CI-UPs as part of the pilot. As a result of the activities, both entities involved in the pilot committed to undertaking measures to improve their cyber security posture. These activities also strengthened the connections between ASD and CI personnel, and improved their collective familiarity with the networks involved.

Reforms to protect CI-SONS

The Committee provided advice to the former Minister for Home Affairs on the development and implementation of 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 former Government. These primarily focussed 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
- clarifying Government Assistance intervention powers
- considering the future inclusion of other assets in critical sectors.

The Committee also provided advice on the importance of government being an exemplar in best practice for cyber security. While the legislative reforms for critical infrastructure, and compliance with them by industry are of vital importance, industry needs to see visible signs that government is hardening its own critical systems. In many sectors, critical infrastructure is guided by governments, not just the private sector.

Bolstering law enforcement capabilities

The National Plan to Combat Cybercrime (the National Plan) was publicly released on 21 March 2022. The National Plan complements existing strategies, including the Ransomware Action Plan and the National Strategy to Fight Transnational, Serious and Organised Crime.

The National Plan works to build a strong operational response to cybercrime. It focuses on strengthening public-private partnerships and providing better support to the victims of cybercrime through the development of a Cybercrime Action Plan and the establishment of a National Cybercrime Forum.

The Joint Policing Cybercrime Coordination Centre (JPC3) was concurrently launched on 21 March 2022 to support the implementation of the National Plan to Combat Cybercrime.

The $89.9 million JPC3 expands the AFP's multi-disciplinary cybercrime investigation teams across Australia. These teams are comprised of investigators, intelligence analysts and technical specialists. The expansion supports 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 worked to build coordinated and collaborative local, national and international policing efforts to counter the increase in cybercrime and cyber threats.

Cybercrime is costly! Especially when personal information is compromised. On average, IDCARE clients report losses of $23,830 AUD following the compromise of a tax file number.[1]

ASD, through its ACSC, hosts officers from the AFP and the Australian Criminal Intelligence Commission (ACIC), to fight cyber crime through integrated teams.

ASD has delivered a number of successful offensive cyber operations through this integrated approach.

Domain Takedown Service

The Domain Takedown Service, launched in March 2021, removes websites or services hosting malicious software. During the 2021-22 financial year, ASD issued almost 62,000 adverse website takedown notifications, helping to prevent cybercrime and fraud.

New powers to combat serious online criminal activity

The *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* commenced on 4 September 2021. It provides three new powers to the AFP and ACIC to help combat serious online criminal activity. These are part of Australia's response to the challenges posed by the increasing use of the dark web and anonymising technologies, which allow criminals, including terrorists and other malicious actors, to hide from law enforcement. They include 'fit-for-purpose' powers and capabilities to discover, target, investigate and disrupt cyber-enabled crime, including on the dark web.

The Committee has provided Government advice and an industry perspective on the development of a national approach to combating cybercrime and improving operational capabilities. The Committee's advice informed the development and successful release of the National Plan to Combat Cybercrime.

In its advice, the Committee emphasised the importance of leveraging new and ongoing partnerships with industry to provide insights on emerging cyber threats and facilitate early disruption of malicious cyber activities. Building partnerships with industry will support agile responses and minimise harmful impacts on members of the community, particularly when protecting vulnerable users of technology and the Internet.

Improve threat information sharing

The Committee will continue to work with Government to advise on co-design and implementation of threat intelligence sharing platforms and cooperation of industry partners including the telecommunications, financial, energy, higher education and research, cloud and defence industry sectors.

In November 2021, ASD launched the CTIS platform, which aims to uplift the real-time sharing of actionable threat intelligence between government and the private sector. As of June 2022, more than 30 partners had been on-boarded to the platform. Of these partners, half are sharing threat information bidirectionally.

ASD also provides a Protected Domain Name Service (AUPDNS) for government agencies, which blocks known 'bad' domains or malicious actors.

1 IDCARE July 2022 Monthly Report

Over the 2021-22 financial year, AUPDNS has blocked more than 180,000 unique known malicious domain names across government agencies.

Following extensive consultation, on 25 November 2021 the *Telecommunications (Interception and Access) Amendment (2021 Measures No. 1) Regulations 2021* were introduced. This regulatory amendment supports the telecommunications industry in its implementation of threat blocking technology designed to protect the public from malicious SMS scams, which impact the operation and maintenance of telecommunications systems.

Telstra blocked more than 200 million scam SMS in the three months up to 31 July 2022, and currently blocks 1,500 scam SMS per minute by leveraging the legislative amendments.

The Committee is of the view that notwithstanding the progress made in threat sharing, further progress needs to be achieved. Threat sharing is the key to identifying malicious activity, which is the key to threat blocking. The development of the government's threat sharing program was a protracted process. Now that the resulting CTIS platform is established, more resources should be dedicated from both the private sector and government to onboard partner organisations quickly and seamlessly'.

Support to victims of cybercrime

Victims of cybercrime often express dissatisfaction with the responses they receive from government, banks, and local police. It can be hard to know what support is available and how to access it. The government funds victim support services through IDCARE.

By providing case management and Cyber First Aid services, IDCARE helps Australians and subscriber organisations to build resilience and receive the assistance necessary to recover from the impacts of cybercrime.

"IDCARE is Australia and New Zealand's national identity and cyber support service. We are a not-for-profit charity that was formed to address a critical support gap for individuals confronting identity and cyber security concerns. This gap requires specialist Identity & Cyber Security Case Managers and Analysts that apply a human-centred approach to identity and cyber security. This means we place at the centre of everything we do the concerns and needs of the individual, not the technology or process."[2]

IDCARE provides a number of specialist services, including:

- case management and counselling to Australian victims of cybercrime
- providing customers with a tailored response plan, a specialist case manager and a premium support service if referred by a subscriber organisation.

IDCARE does not charge individual community members for base support services. It is funded by subscriber organisations such as the Department of Home Affairs (Home Affairs), grants and cost recovered services.

2 About IDCARE - Not for profit organisations

In January 2021, the former Government signed a contract with IDCARE to provide up to $6.1 million over four years to support Australian victims of identity theft, scams and cybercrime by providing specialist support to incident recovery and mitigation. This funding enables IDCARE to deliver increased support services, and provide government with regular reporting on emerging threats and identity exploitation trends.

IDCARE completed 9,226 case management cases for the Commonwealth within the first five months of the contract (January – May 2021) with a total of 21,313 case management cases completed under the contract in the 2021 calendar year.

The strong demand for support services experienced by IDCARE demonstrates the extent of cybercrime and identity theft, and its substantial impact on Australians.

24/7 Hotline

On the 25 November 2021, the ASD launched the enhanced Australian Cyber Security 24/7 Hotline. The expanded hotline is designed to support small-to-medium businesses, individuals and families, and included an upgrade to both technical capabilities and increased staffing.

During the 2021-2022 financial year, the ASD responded to over 25,000 calls to its Cyber Security Hotline – an increase of more than 15% from the previous financial year.

A cyber skilled workforce

A strong and capable workforce of skilled cyber security professionals is a key enabler of Australia's digital economy and national security. Greater effort is required to reduce this critical shortage, including by bolstering the pipeline of entry-level roles in cyber. The Strategy funds initiatives and programs to upskill and provide a point of entry into cyber for early and mid-career professionals.

Despite recent gains in increasing diversity in our digital technology sectors, there is opportunity for improvement. As reported by AUCyberExplorer, nation-wide there are an estimated 107,909 male and only 35,802 female workers in the cyber security workforce.[3]

In addition to short and medium term initiatives to grow the workforce, the Government is committed to uplifting Australia's economy and expanding the skills pipeline. Programs such as Questacon's Cyber Program have a key role to play by fostering interest and knowledge in teacher and school-aged students.

The Questacon Cyber Program engages young Australians and educators to build foundational skills that underpin professional cyber security practices. The program was designed following a discovery process identifying a national need for more cyber education opportunities for teachers and primary school students.

Questacon's activities strongly align to the Australian Curriculum Digital Technologies and Digital Literacy outcomes, and have been piloted with 361 teachers and 738 primary school students across Australia since 2021.

3 AUCyberExplorer

Comprehensive evaluation of the Questacon Cyber Program's pilot programs demonstrates how they can increase the number and diversity of school students being equipped and motivated to become our cyber security workforce of the future:

- Amongst students, initial results show that after Cyber Design Challenge workshops more than 70% wanted to learn more about cyber outside of the classroom, regardless of year level or gender identity.
- Amongst teachers, most Cyber Squad participants reporting improved confidence to integrate cyber content into curriculum and lesson planning. Numbers who 'strongly agreed' or 'agreed' increased from <30% pre-workshop to >60% post-workshop. Teacher confidence to teach the Digital Technologies curriculum similarly increased.

Building on these pilot program outcomes, Questacon's ambitious National Cyber Design Challenge will reach a significantly increased audience using a scalable digital platform. A custom world built in Minecraft: Education Edition will engage students with cyber security concepts while exploring a 'castle defence' cyber threat.

Other initiatives under the Strategy are aimed at developing innovative programs for training and attracting workers of all levels to cyber.

The Cyber Security Skills Partnership Innovation Fund

In 2022, members of the Committee participated in evaluation activities for the Cyber Security Skills Partnership Innovation Fund (CSSPIF), which provides industry and education providers with funding to deliver innovative projects that meet local requirements to quickly improve the quality and availability of cyber security professionals in Australia.

Through the first round of CSSPIF grants, eight successful applicants were awarded a total of $8.2 million in 2020-21. Successful applicants from Round One included:

- Central Regional TAFE, funded $268k for their project on expanding cyber security skills in regional Western Australia
- RightCrowd Software, funded $1.1 million to establish a Gold Coast Cyber Studio
- the Commonwealth Scientific and Industrial Research Organisation (CSIRO), funded $260k for their project Innovate to Grow – Cybersecurity (I2G-Cyber), a free 10-week program for small to medium enterprises (SMEs) to further research and development opportunities related to cyber security solutions.

Round One CSSPIF projects have started their partnerships to increase the quality and quantity of cybersecurity professionals, develop their skills, and improve employment outcomes. For example, Round One participant La Trobe University is working with Australian employers, educators and other partners to expose 71,805 high school Year 9-12 students to cyber security opportunities and education. They are also working together to accelerate the development and delivery of experiential work based learning that is backed up with micro-credentials.

La Trobe's early achievements include:

- a series of cyber expert virtual workshops and speakers with Quantum Victoria and Cisco
- cyber security micro subjects and a pilot career transition program
- recruitment webinars and alumni promotions
- specialist online modules for gifted and talented students
- early engagement with the AFP, NBN Co, Fujitsu, QBE, the Australian Competition and Consumer Commission and Australia Post on micro credentialed learning.

The ADF Cyber Gap Program

The Australian Defence Force (ADF) Cyber Gap Program is a 12-month online program undertaken in conjunction with tertiary study. Its objective is to enhance the cyber skills and employment opportunities for graduates.[4]

Applications for Intake Two of the Program opened on 1 September 2021 and closed on 31 October 2021, with over 1,200 applications received. The program is on track to sponsor 800 participants by December 2023.

ASD's workforce initiatives

ASD has progressed a number of cyber workforce initiatives including sponsoring the Australian Women in Security Network (AWSN) and Australian start-up OK RDY, to develop the Women in Security Mentoring Program pilot. The pilot had 110 participants by May 2022 and is due for public launch in August 2022.

In addition to the mentoring program, ASD's Women in Cyber initiatives in the 2021-22 financial year continue to support women to undertake and progress careers in cyber security, including:

- InfoSect Technical Training Scholarships for 30 women in reverse engineering, code review and network security
- sponsorship of public presentation coaching for women to present at cyber conferences for the first time
- sponsorship of CyberTaipan 2022, an Australian youth cyber competition for primary students
- sponsorship of student career fair, Go Girl, Go for IT 2021-22, targeted at ages 10-17
- AWSN sponsorship 2021-22 for 100 women in the Security Pathways Program and 110 for the Women in Leadership Program
- sponsorship of the Australian Women in Security Survey conducted by RMIT
- partnership with GROK Academy for student cyber challenges and camps
- outreach to secondary students with ASD CyberEXP, a gamified, interactive online cyber career tool
- sponsorship of the Canberra node of Girls Programming Network (GPN), a quarterly coding workshops for girls aged 10-17.
- and consumers.

4 Australian Defence Force Cyber Gap Program | Digital Profession

Supporting Women in Cyber

In 2021, ASD partnered with the Australian Women in Security Network (AWSN) and Australian start-up, OK RDY to deliver the 'Women in Security Mentoring Program' 12 month pilot. Over 100 AWSN members participated in the pilot and created real connections, deeper mentoring engagements, expanded their networks and participated in mentor and mentee training. The #MentoringMatters app that underpins the program utilises state-of-the-art technology and artificial intelligence designed by OK RDY for optimum mentor and mentee matching, with the ability to expand, adapt and scale to offer the best possible experience for women as they pursue their mentoring journeys.

Participants reported greater fulfilment and connection to their roles, with some winning career promotions. Following the pilot success, an expanded and improved app and ongoing mentoring program will launch in August 2022 to connect more women with mentors. This will continue to increase women's participation in security roles, build networks, and grow workforce capabilities in the Australian security sector. The national program is expected to expand to support over 1000 women in its first year. Under AWSN's ownership from 2024, the program will grow to offer mentorship to other underrepresented communities within the security industry beyond the end of government funding in 2023.

The Committee welcomes the Government's election commitment to grow the tech-related workforce by 1.2 million jobs by 2030. The shortage of appropriately skilled cyber security professionals continues to have a negative impact on Australia's ability to prevent and respond to cyber security incidents and more needs to be done to grow the workforce and promote diversity in cyber and critical technology.

The Committee's advice also highlights the need to build the skills pipeline of entry level roles in cyber and shape the pipeline for industry through Government leadership. The Department of Education and the Jobs and Skills Agency should encourage and assist Australia's educational institutions to build more basic cyber skills in a broader range of curriculums such as software engineering, robotics and other tertiary programs. The Committee emphasised that while deep cyber specialists are important, Australia also needs to better equip a broader range of technologists.

Joint Cyber Security Centres (JCSCs)

ASD is enhancing the capability and maturity of JCSCs across Australia to assist businesses and critical infrastructure providers. Initiatives include:

- expansion of the JCSC workforce (including Home Affairs outreach officers)
- upgrades to ICT and facilities
- expansion and tiering of the ASD partnerships program.

Over the last year, ASD has continued to grow its JCSCs. In cooperation with the Northern Territory Government a new virtual JCSC office has been established in Darwin, improving support to businesses in the Northern Territory. Tasmanian businesses are supported by a JCSC engagement officer and a Home Affairs outreach officer in Hobart, Tasmania.

Throughout the 2021-22 financial year, the JCSCs continued to offer support to industry and government partners, including tailored advice and cyber threat intelligence briefings. In the 2021-22 financial year, the JCSCs hosted more than 370 cyber security technical events. For example, the ASD has delivered six cyber security exercises with critical infrastructure owners and operators, through the JCSCs.

Cyber and Infrastructure Security Outreach Officers

Continuing the Strategy's commitment to strengthen industry partnerships, Home Affairs is continuing to roll out a network of cyber and infrastructure security outreach officers. These outreach officers are embedded in the JCSCs to bolster industry engagement across Australia, particularly focused on SMEs, providing those entities with advice and assistance to uplift their security and resilience, with a key focus on cyber preparedness and protection.

The outreach officer network is focussed on engaging with businesses at scale to maximise impact, operating as part of ASD's JCSCs. The network uses peak bodies to serve as a conduit to inform industry of Commonwealth initiatives, programs and advice, and receive feedback on business needs.

During 2021-2022, the Cyber and Infrastructure Outreach Network collaborated with the Australian Taxation Office (ATO) for their Small Business Newsroom. The outreach team provided cyber security information and advice for their 3.1 million subscribers, mostly small business operators.

The team worked with the ATO and provided an article on Business Email Compromise (BEC) scams for the January Small Business Newsroom newsletter (distributed electronically and published online).

The article amplified recent ASD alerts noting the increase in BECs and encouraging businesses to exercise vigilance and adopt key mitigations. It directed readers to ASD small business and cyber resources available.

To supplement this, the outreach team followed up with a cyber-security awareness webinar for small business operators. The webinar covered common threats and scams, measures to support cyber uplift and resilience, and amplify key resources available at cyber.gov.au. Feedback was positive, and the team will seek to engage with the ATO's extensive small business cohort again.

The Committee is of the view that effective and deep engagement between government and industry and across government is crucial to lift our cyber defences. The JCSCs, which were an initiative under the 2016 Cyber Security Strategy, are one of the key vehicles to facilitate this.

Furthermore, the JCSCs are an important resource, particularly in the nexus between industry and government and across government. After a too protracted launch process, the JCSCs are now fully established. To grow their strategic utility, the JCSCs should seek to deepen industry integration opportunities with subject matter experts. REDSPICE presents a clear opportunity in this respect, where industry and government operational experts could co-locate in capital cities and tackle shared projects and problems.

Notwithstanding this progress, the Committee recommends more needs to be done to accelerate the development of the JCSCs as a key vehicle for government and industry partnership.

ACSC Partnership Program

ASD's ACSC **Partnership Program** facilitates ASD engagement with a broad range of Australian organisations and individuals to lift cyber resilience across the Australian economy. The program comprises three tiers of partners: Network Partner, Business Partner and Home Partner.

- The Network Partner tier includes cyber security professionals across government, industry, academia and the research sector.

This tier allows the public and private sectors to support and learn from each other, sharing insights and collaborating on shared threats and opportunities.

- The Business Partner tier consists primarily of SMEs. Membership of this tier provides these organisations with access to products to build their awareness of the cyber security landscape as well as advice to protect them against cyber threats. The Home Partner tier is for individuals and families who would like to subscribe to the ACSC Alert Service, providing them with a better baseline understanding of the cyber security environment.

During the 2021-22 financial year, the Partnership Program delivered more than 90 sector specific activities, with approximately 1700 attendees across the events.

Supporting SMEs

ASD has created tailored guidance to equip small businesses with the information and tools needed to protect themselves from cyber security threats. This information is available online at cyber.gov.au and includes:

- ACSC's **Small Business Cyber Security Guide** which provides actionable cyber security advice tailored to small businesses
- **Step-by-Step Guides** which are practical handbooks with steps and visual aids for small businesses to implement essential cyber security measures such as automatic updates and backups
- **Quick Wins** which are quick summaries providing practical actions and considerations to improve small business cyber security, such as guidance on unsupported software.

The ACSC's Alert Service provides easy-to-understand online security information and solutions to help protect internet users at home, at work and on mobile services. The ACSC Alert Service also informs users about the latest threats and vulnerabilities within an Australian context, and how to address risks to their devices or computer networks. Alerts are publicly available on cyber.gov.au. Interested parties can subscribe to receive alerts, and organisations can receive alerts as Partners under the ASD Partnership Program.

Between July 2021 and June 2022, the ACSC published 24 new or revised technical cyber security guides tailored to small businesses and individuals.

The Connect and Protect Program

In October 2020, the former Government launched the Cyber Security Business Connect and Protect Program to support 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.

Led by the Department of Industry, Science and Resources (DISR), the program included the release of a Cyber Security Assessment Tool[5] 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.

Exploring options to uplift the cyber security of Australian businesses and across the digital economy continues to be of vital importance to Australia's economic future. The role of privacy and consumer protection, safety by design principles, supply chain management and corporate governance will need to be considered.

5 https://business.gov.au/news/is-your-business-cyber-secure

Online learning platform

In October 2021, the ACSC released online learning resources on cyber.gov.au to support Australian small businesses, Australian individuals and families. These resources are designed to provide users with practical, actionable approaches to prepare for and prevent cyberattacks. They are tailored to each audience and in a format accessible to a broad range of the Australian community.

Enhanced incident response

During the 2021-22 financial year, the ACSC responded to approximately 1,100 cyber security incidents. The ACSC continues to support Australian businesses and organisations by providing timely and updated advice on cyber security incidents, for example, advice on the Log4j vulnerability. By partnering with industry sectors, such as banking and telecommunications, ASD tailors advice on mitigating key vulnerabilities to stakeholders.

Greater cyber security preparedness and mitigation strategies across government and industry domains remain a primary interest for Government. The National Exercise Program (NEP) runs scalable and agile exercises to help participants validate and improve their cyber security incident response. The exercises are controlled activities that use a scenario to simulate a real-life cyber security incident. NEP also regularly runs cyber security training workshops for industry and government.

In August 2021, ASD delivered AquaEx, a national exercise to strengthen Australian industry and governments' coordinated response should a cyber incident affect Australia's critical water and wastewater sector. The AquaEx series of exercises included an operational level exercise involving 760 personnel from 48 organisations, and a strategic level exercise involving 36 personnel from 22 water and government organisations. AquaEx provided participants with valuable insight into government agencies' preparedness to respond to a significant cyber incident in the sector, and presented opportunities to strengthen current arrangements.

Awareness raising

The need for an integrated national approach and a cohesive single voice from government has been a key point of feedback from the Committee and has informed the development of awareness raising campaigns under the Strategy. Home Affairs and ASD are working to uniformly message cyber.gov.au as the sole user-entry point.

Act Now, Stay Secure

In November 2020, the ACSC launched its 'Act Now, Stay Secure' cyber security awareness campaign for all Australians. The campaign has focussed on providing effective messaging to various at-risk communities including small businesses, older Australians and families, with the key publications made available in a range of languages to reach culturally and linguistically diverse (CALD) audiences.

The initial emphasis of the campaign was on prevention and recovery from ransomware. It has since evolved to provide additional advice, including back-ups and updates, setting strong passwords, securing personal devices and multifactor authentication.

Over the course of the campaign, monthly themes have provided opportunities for the ACSC to deep dive various cyber security topics. The information seeks to provide understandable, practical advice supported by a suite of resources.

Beat Cybercrime in Your Downtime

Home Affairs' public information campaign 'Beat cybercrime in your downtime' was launched on 31 October 2021 and reached large sections of the community (particularly vulnerable Australians) with a perspective-changing message to help individuals enhance their personal cyber secure behaviours. Research conducted to inform the campaign indicated increased national cyber security resilience begins with individuals, whose actions cascade across the whole of the economy.

Home Affairs collaborated closely with the ACSC, who provided technical expertise, as well as other Commonwealth agency partners and the Committee to share research and audience insights during development. This campaign complemented ASD's 'Act Now, Stay Secure' digital campaign and promoted cyber.gov.au as the trusted source of information and advice.

For target audiences, it revealed the campaign was successful in shifting attitudes and perceptions of the importance of cyber security and managing cyber security threats:

- 69% of Australians who saw the campaign took action as a result, such as implementing multi-factor authentication. This was significantly higher among Aboriginal and/or Torres Strait Islanders, with 86% taking action.
- Campaign recognisers reported feeling more confident and in control of their cyber security.
- Digital channels achieved more than 13 million video views with over 248,000 clicks to the campaign website.
- The campaign ran content in multiple languages to reach CALD audiences. The CALD YouTube activity performed extremely well and exceeded benchmark targets.

The campaign also significantly increased traffic to and raised the profile of cyber.gov.au, which will assist ASD to deliver cyber security advice and education long after the campaign's conclusion.

What these initiatives demonstrate is the critical importance and impact of increasing awareness of cyber risks and what individuals can do to protect themselves. While many cyber-attacks are technologically sophisticated and persistent, it is very often the case that by adopting a few basic and simple principles and practices, potential victims can protect themselves: Do not click the link, maintain off-line backups, manage your passwords, and be aware of personal information online.

The Committee is therefore of the strong opinion that more needs to be invested in awareness raising to amplify and reinforce the good work and messages already communicated.

The Committee provided advice to Government on the need to continue ongoing campaigns to raise cyber security awareness in the community. Evaluation of the effectiveness of the awareness raising campaigns, particularly to ensure they measure the cyber awareness of businesses and individuals, should be an ongoing priority.

The Committee has also advocated for the use of social media as an effective means to tailor messages. The Committee has emphasised social media's ability to amplifying awareness campaigns for small businesses, to ensure they know how to protect the data of their business and their customers. Further, the Committee notes that 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 overall cyber security uplift.

International Cyber and Critical Technology Engagement Strategy

On 21 April 2021, the International Cyber and Critical Technology Engagement Strategy (International Strategy) was launched. 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 Australia's Cyber Security Strategy 2020 and other government initiatives, producing a cohesive domestic and international approach to developing cyber resilience and tackling issues of cross-border cyber threats.

The Cyber and Critical Tech Cooperation Program (CCTCP) reflects the three pillars of the International Strategy and provides a framework for partnership with Indo-Pacific countries, as well as supporting Australia's commitment to deliver on the United Nations 2030 Agenda for Sustainable Development. Action is underway across the full range of objectives, covering Australia's values, security and prosperity.

Programs delivered in 2021 under the CCTCP include:

- the Women in International Security and Cyberspace Fellowship Network, which continued to support greater participation of women at the United Nations
- the ASD-led Pacific Cyber Security Operational Network, which supports the collaboration and sharing of cybersecurity threat information, best practice tools, and techniques to manage cyber incidents
- the AFP-led Cyber Safety Asia and Cyber Safety Pasifika programs, which supported development of improved cybercrime investigative capability in Southeast Asian and Pacific States
- uplifting cyber capability through the Cyber Bootcamp training courses.

Since the launch of the International Strategy, there has also been progress in furthering international law and norms of responsible state behaviour in cyberspace. Australia has engaged closely with partners in Southeast Asia and the Pacific to achieve these aims. In 2021, workshops were convened in ASEAN states to build understanding of how to operationalise these norms.

Australia has also deepened its relationships with partners in the Indo-Pacific on cyber security matters. This includes through projects such as the Pacific Islands Law Officers' Network, which runs an annual cybercrime workshop led by the Attorney-General's Department and co-funded with the Council of Europe, and working with the United States, India and Japan in the context of a Quad working group on Critical and Emerging Technology.

Evaluating Progress of Australia's Cyber Security Strategy from 2020–2022

The Committee considers evaluation of the Strategy to be a necessary, useful and key component of identifying the effectiveness of government investments, informing gaps and issues for future initiatives, and strengthening Australia's national resilience.

While the initial program outcomes indicate that Australia's cyber security posture has been significantly improved as a result of the Strategy's initiatives and programs, the development of a strategic maturity evaluation framework, underpinned by more rigorous data, empirical analysis and measurements, will allow Australia to confidently and continually examine the impact of the Strategy in uplifting the cyber security of the Australian government, businesses and the economy, and the Australian community.

To date, programs have primarily focussed on increasing government, business and community accessibility and uptake of cyber security advice. This has included addressing part of the cyber skills gap by attracting and training new cyber talent, delivering support services to cybercrime victims and developing additional best practice guidance to government and industry stakeholders. More details can be found in **Appendix C**.

Strategy's Impacts on Industry

The initiatives and programs focussed on industry aim to assist businesses to protect themselves, their supply chains and their customers from cyber threats. These programs work towards this goal by uplifting the security of critical infrastructure and SMEs, securing the Internet of Things, increasing the cyber-skilled workforce and blocking threats automatically to prevent them reaching businesses and consumers.

Work to date has also laid the groundwork for improved data collection, and building Australia's understanding of the workforce needs and skills gaps in our national economy relating to cyber.

Under the Cyber Security National Workforce Growth Program, DISR was allocated $2.5 million to improve data collection on cyber skills shortages to ensure policy makers delivery informed and evidence-based solutions for future skills demands. These programs are all on track or have been delivered to support cyber workforce uplift. This includes working with:

- the Australian Bureau of Statistics (ABS) to update the Australian and New Zealand Standard Classification of Occupations (ANZSCO) to better reflect cyber security and related occupations

- the Behavioural Economics Team of the Australian Government to research people's decisions in relation to working in cyber security
- the Australian Strategic Policy Institute to research the cyber security sector products, technologies, skills and capabilities needed to protect Australia's national interests.

ANZCSO update to facilitate more comprehensive data collection

Released on 23 November 2021, DISR worked with the ABS to update the ANZSCO cyber security occupations to better reflect changes in technology and market labour movements. The update included seven new six-digit level cyber security occupations and eight new specialisations in ANZSCO to facilitate more comprehensive data collection.

The new ANZSCO classifications enable better analysis of the cyber security industry's workforce and growth. The 2021 update to the ANZSCO cyber security related occupations allows for a more granular level of workforce composition and skills data to be collected. The ANZSCO update is also being used to align to new cyber security skills shortage data reporting and forecasting platform upgrades, including AUCyberExplorer.

Overall, program leads reported an increase in the willingness and ability of businesses to take responsibility for securing their products and services, and protecting their customers from known cyber vulnerabilities. However, the COVID-19 pandemic impacted the delivery of some programs. For example, the Questacon Cyber Program was forced to move to an online delivery model.

The Strategy's Impact on our Community

The Strategy's programs have included targeting the Australian community through targeted engagement, educational programs and the provision of best practice guidance to increase cyber security awareness among individuals and SMEs and provide additional avenues for them to seek help.

Program leads reported at least a moderate increase in both Australians' cyber awareness and the accessibility of support resources, with most participants reporting significant impacts on their target audiences. Outcomes mostly relied on the quality and quantity of stakeholder uptake in the programs and any positive measurable changes in behaviours.

The community is particularly vulnerable to the cyber threats, and these programs sought to mitigate these risks by providing easily accessible, digestible and tailored resources.

For instance, continued support was provided to IDCARE to ensure Australia can keep up with the increasing demand for support services by victims of cybercrime.

While IDCARE support is a reactive government measure to individuals already being targeted by cybercriminals, the 'Beat cybercrime in your downtime' and 'Act Now, Stay Secure' cyber security awareness campaigns led by Home Affairs and ASD respectively aimed to prevent them from being targeted.

The campaigns' effectiveness were measured by the level of public engagement and resulting cyber secure behaviours. Between January and February 2022, surveys of participants who had completed online learning on cyber.gov.au measured the overall effectiveness and uncovered insights about user behaviour and attitudes, intention and platform experience. Results indicated that the likelihood of all users accessing a government website for cyber security information significantly increased after they visited the platform (15% increase of at-risk & family users and 16% increase of small to

medium enterprise users). Further, 90% of at-risk & family users and 84% of small to medium enterprise users reported that they would take online security more seriously after visiting the ACSC online learning resources. In November 2021, the ACSC social media channels posted 12 times about the online learning resources, potentially reaching over 67,000 users with an engagement rate of over 3.1% and click through rate to cyber.gov.au/learn of over 1.3%.

These metrics are in line with ACSC's average engagement rates and are well above Industry benchmarks.

The Strategy's Impact on Government

The programs under the government cohort of initiatives focus on uplifting the cyber security of government agencies and critical infrastructure, as well as increasing cooperation with all levels of government, international partners, law enforcement, industry and academia.

CYBER HUBS

As the Australian Government's IT networks become more interconnected, a centralised approach to modernising cyber security is essential to keep pace with the evolving threat environment. As a first step, establishment of Cyber Hubs is currently being piloted as an initiative under the Australian Cyber Security Strategy 2020.

Commencing on 1 July 2021, the Cyber Hubs pilot is testing a whole-of-government approach to monitoring, detecting and responding to cyber threats across government.

During the first year or the pilot (2021 22) Cyber Hubs have been established in Home Affairs, Defence and Services Australia, with on-boarding commencing for six client entities:

- Australian Criminal Intelligence Commission (ACIC)
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Australian Civil Military Centre
- Australian Hydrographic Office
- Sport Integrity Australia
- Australian Digital Health Agency.

Delivery of consolidated core cyber security services to these client entities is being tested successfully in a live production environment and have shown potential to substantially improve client entities' cyber security.

The current Cyber Hubs pilot will continue through to 31 December 2022. Learnings from the initial phase of pilot implementation, including a formal 6 month mid-point review, are shaping the focus for the rest of the pilot. Key deliverables for the rest of the pilot include:

- standing up an additional Cyber Hub in the Australian Taxation Office
- preparing on-boarding readiness assessments and transition plans for all remaining Non-corporate Commonwealth Entities
- conducting an evaluation of the pilot.

The outcomes of government programs were mainly measured against the quality and quantity of stakeholder accessibility and uptake, the reduction of harm to Australians and our national interests and the passage of legislation or regulatory reforms. These measures included the amount of activities from cyber criminals which were disrupted, the number of engagements with industry and community, and the passage of supporting legislative reforms.

The Committee continues to emphasise the need for a robust, useful and fit-for-purpose evaluation and measurement process to ensure the Strategy delivers effective outcomes, assists the Committee in providing quality advice to Government, and identifies risks and opportunities for future programs.

The Committee's work

The Committee holds quarterly meetings, to receive updates and advise on the Strategy's implementation, consider new and emerging issues in cyber security, and provide industry and academia with insights on the impact of legislative and regulatory changes.

In addition, the Committee has held roundtables, workshops and deep dives on key issues such as directors' duties and the Essential 8. It has also met with sector-specific representative groups, including on cyber insurance with the insurance industry.

The Committee Chair has also met with key agencies and experts internationally to exchange best practice information in cyber security. In the US, these include the US President's National Security Telecommunications Advisory Committee, the Cybersecurity and Infrastructure Security Agency, the White House, the Federal Bureau of Investigation, the National Security Agency, as well as the Government Communications Headquarters and the National Cyber Centre in the UK.

The Committee has helped to shape key initiatives under the Strategy. These include the review of the reforms for the protection of CI-SONS, development of recommendations for businesses and the economy, and community awareness campaigns.

The Committee has considered the implementation of the Strategy, informed by briefings from relevant government departments and deep dive discussions.

The Committee looks forward to working with the new Minister for Cyber Security.

Committee's advice on cyber security issues over the year

Throughout the 2021-22 financial year, the Committee provided advice and perspectives 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
- new opportunities and emerging challenges presented by the rise of cryptocurrency.

Hybrid Work thought-piece

On 17 November 2021, the Committee published its second thought-piece entitled *Back to Business: Recognising and reducing cyber security risks in the hybrid workforce*.

This paper highlights the key cyber security issues facing Australian businesses – big and small – as the country emerges from the COVID-19 pandemic including ensuring Australia's post-COVID hybrid workforce is cyber secure.

More Australians than ever before desire a shift to hybrid work. While there are financial, work satisfaction and productivity gains this shift promises, there are also risks such as an increased cyber security vulnerability. Therefore, Australian organisations require practical advice and assistance in making the hybrid shift, with cyber security in front of mind.

Organisations of all sizes seeking to implement hybrid working practices need to have the correct processes in place to bolster the cyber security of a dispersed workforce.

While there is no one-size-fits-all model for organisational cyber security, it is important for organisations to have the basics right, in addition to some specific actions that can be taken to bolster cyber security for hybrid workforces.

This thought-piece provides practical information for organisations transitioning to long-term hybrid working, including:

Know what to protect across the hybrid environment

- Understand the critical areas to business continuation and focus security investment decisions in these areas.

Revise corporate policies so they are fit for purpose in a hybrid world

- Make sure policies are clear and explicitly communicate how and where work devices can be used.

Get the basics of cyber hygiene right

- Focus on cyber hygiene basics – educate people, ensure consistent patching and updates, use multi-factor authentication, use passphrases and keep back-ups of resources.
- Know what resources are available and where to find them, such as cyber.gov.au.
- Educate staff about cyber security, with a specific focus on the risks that increase through working hybrid. Make staff education human-centric, real-time and interactive.
- If staff have connectivity issues, make sure they do not use unmandated devices or networks to connect (e.g. public wi-fi, personal dongles).

Leverage innovation and build in security upfront

- Integrate cyber security uplift into hybrid workforce business innovations.
- Make the shift easier for staff by making intuitive cyber security a part of basic processes. For example, introduce biometric multi-factor authentication so that staff do not have to remember multiple passphrases.

Small and Medium Enterprises (SMEs)

- Choose products and services that easily enable continual cyber security updates.
- Optimise the benefits and incentives that may be available by working with an accountant or financial team (e.g. if tax incentives like instant asset write-offs can be used to uplift cyber security).
- See if there are cyber uplift subsidies or grants available.

Large Businesses and Corporations

- Identify staff members more likely to be targeted by cyber criminals (e.g. CEOs, executives, accounts payable) and conduct at-home cyber security assessments.
- Consider the introduction of a 'cyber allowance' for hybrid workers to support the strengthening of home networks.
- Identify and shut down legacy technology.

Individuals

- Be part of the team – attend and actively engage in cyber security training.
- Know an employer's cyber security policies for hybrid work and stick to them.
- Be aware of online activity and make sure to separate work from recreation.
- If an email or other online interaction does not seem quite right, refer it to the security team.

Cryptocurrency thought-piece

The Committee's third public thought-piece was published on 2 March 2022 with a focus on cryptocurrency.

This paper explores the opportunities alongside the cyber security and cybercrime implications of cryptocurrency and how these risks could be better mitigated for Australians. In particular:

- what cryptocurrency is
- the risks associated with cryptocurrency
- the nexus between cryptocurrency and crime
- the current state of domestic and international cryptocurrency regulation
- the opportunities cryptocurrency presents.

The recommendations in the paper provide some forward-facing steps to help foster the secure adoption of cryptocurrencies in Australia, address crypto-related crime, as well as support crypto-driven opportunities in Australia. These include:

- the consideration of mandated minimum cyber security standards for registered digital currency exchanges (DCEs) and businesses that hold crypto assets operating in Australia. However, this must be a shared responsibility and businesses using cryptocurrencies should also take appropriate steps to ensure strong cyber security measures are in place.
- properly resourcing industry, government, law enforcement, regulatory and criminal intelligence agencies to meet the demands of the complex digital world. There should be a focus on increased specialist training about the nexus between the cryptocurrency opportunities and cybercrime and increased public awareness messaging about how cryptocurrency can facilitate crime.
- coordinating more purposefully with like-minded nations to ensure 'breaking the chain' work is coordinated, tax evasion is managed and International Funds Transfer Instruction (IFTI) reporting is implemented to track the movement of illicit funds and related penalties. Australia should follow the example of countries leading the way, learning from their experiences, and coordinating international best practice with respect to cybersecurity in cryptocurrency.
- increasing transparency around registered DCEs and providers of blockchain-based financial products or services that hold AFSLs to boost consumer confidence in using and investing in cryptocurrency. Educational programs with accurate, consistent messaging will allow investors to better understand both the investment and cybersecurity risks while helping to demystify cryptocurrencies for all Australians.

The Committee's fourth thought piece is due to be published in October 2022.

Developments in the Threat Environment

The global cyber threat environment has intensified over the last twelve months and Australia is, and remains, an attractive target for malicious actors and cybercriminals. New technologies and the move to more time spent online, as a result of the COVID-19 pandemic, have created greater opportunities for cybercriminals.

Geopolitical tensions have been significantly exacerbated following Russia's invasion of Ukraine, and the risk of attacks on Australian networks – whether directly or inadvertently – has increased. While the threat of attack by state actors is very real, the knock-on effects of these tensions that represent the greatest danger to consumers. Malicious actors and cybercriminals look to take advantage of the vulnerabilities exploited by state actors, and critical infrastructure networks will continue to be targeted by both state actors and criminal syndicates. Following the invasion of Ukraine, there is a heightened cyber threat environment globally.

Social Engineering

Social engineering remains one of the most prominent and successful techniques employed by cybercriminals. By preying on human error rather than technical vulnerabilities, criminal actors continue to circumvent existing security arrangements put in place by businesses and organisations. An example of one of the more novel forms taken are Deep Fakes, which are rapidly gaining in popularity. More sophisticated than a simple phishing email, they use artificial intelligence software to create fake videos, images, or audio recordings of real people. Social engineering will continue to evolve to incorporate new trends, technologies and tactics.

Business Email Compromise (BEC)

BEC is when attackers use email to masquerade as legitimate business, sending messages which are designed to deceive recipients into sending money or goods to the attacker. Prominent examples include invoice fraud, impersonation and gift card scams, but BEC ploys can take many forms.

Cybercriminals conducting BEC leverage topical events and issues, like the COVID-19 pandemic, to exploit victims' sensitivities and fraudulently coerce them into providing money or goods to a 'cause'.

BEC is now the most financially impactful kind of cybercrime in Australia. Although instances of BEC are also almost certainly underreported, the ACSC Annual Cyber Threat Report 2020-21 advised Australians lost $81.45 million to BEC in the 2020-21 financial year.

> From 1 January 2022 to 30 June 2022 there have been over 2,300 suspected BEC incidents reported to ReportCyber.

The establishment of a clear and consistent process for consumers to verify and validate requests for payment and sensitive information is a vital part of blunting the impact of BEC.

The AFP leads Operation DOLOS, an AFP-coordinated multi-agency operation consisting of state and territory police as well as partners from the banking and financial sectors. Operation DOLOS works to target and disrupt the BEC crime model. Between July 2021 and May 2022, Operation DOLOS has recovered approximately $5.2 million lost by the Australian community to criminal elements. In addition, Operation DOLOS has coordinated national and international campaigns and disrupted illicit proceeds by targeting the transnational organised cybercrime syndicates conducting and facilitating BEC schemes.

Ransomware

Ransomware continues to be a significant focus for Australia given the risk it poses to industry and the community. The use of this malware can have significant nation-wide cascading impacts on large sectors of our economy down to individuals. It causes serious operational, financial and reputational harm to victims and can affect any organisation. Globally, without prevention, deterrence and response mechanisms in place, it is estimated that ransomware will cost victims more than $265 billion USD annually by 2031.[6]

In February 2022, a ransomware attack on Bridgestone Corp's U.S. subsidiary, one of the largest global manufacturers of tires, resulted in the company being forced to halt production for a week. This attack occurred just weeks after suppliers of automaker Toyota Motor Corp reported similar attacks.

Cybercriminals continue to leverage social engineering schemes and security vulnerabilities in software and systems to deploy ransomware against victims, while their innate ability to innovate and adapt is driving the development of new extortion methods.

Ransomware tactics are varied and adaptable. Double extortion, a tactic introduced by the Maze ransomware group in 2019 which involves combining traditional encryption with data theft, has grown to become the predominant tactic used by top-tier ransomware operations. In an effort to avoid disruptions that would elicit a strong law enforcement response, some operations have gone as far as extorting victims solely through data. Threat actors have since introduced the use of DDoS attacks and direct communication with customers, stakeholders, and media as additional means to pressure victims into paying ransoms.

In March 2021, the Committee released it's first thought-piece *Locked Out: Tackling Australia's ransomware threat* with further details on the threat posed by ransomware, the policy issues relating to it, such as those relating to the cyber insurance market, and recommendations on what small businesses can do to protect themselves.

From April 2022, the Costa Rican Government has been extensively targeted by internationally-based ransomware actors, resulting in the shutdown of hospital record-keeping systems, an online tax portal and an online payment system for teachers. With the ransomware actors demanding a ransom of $20 million USD, Costa Rica has declared a national state of emergency for the first time.

6 Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 (cybersecurityventures.com)

In May 2022, cybercriminals caused major disruption to IT systems belonging to Costa Rican government agencies, threatening to overthrow Costa Rica's Government if a ransom wasn't paid. In June 2022, another band of cybercriminals also attacked the Costa Rican public health services and systems, causing the affected organisations to shut down their computers to prevent the spread of a malware outbreak.

Australia's Ransomware Action Plan was released in October 2021 to complement existing government lines of effort to combat ransomware, including the Strategy, through three objectives:

- **Prepare and Prevent.** Build Australia's resilience to ransomware attacks.
- **Respond and Recover.** Strengthen responses to ransomware attacks by ensuring support is available to victims.
- **Disrupt and Deter.** Disrupt cybercriminals through deterrence and offensive action, increasing the risk of ransomware gangs being caught.

One of government's operational responses to ransomware recognised under the Ransomware Action Plan is Operation ORCUS. In July 2021, the AFP established Operation ORCUS as an AFP-led multi-agency taskforce comprised of ACIC, ASD, AUSTRAC and state and territory policing partners to coordinate the national law enforcement effort against ransomware, targeting developers and those who utilise 'Ransomware-as-a-Service'.

Through Operation ORCUS, the AFP detected indicators of compromise showing several Australian organisations were being targeted by ransomware attacks. Action was taken to notify impending victims in order to pre-emptively halt attacks and protect victims from financial loss. Operation ORCUS works with international partners, including Interpol and Europol, via a range of forums to address the ransomware threat, including analysing hundreds of ransomware incidents, preparing and distributing intelligence reports and conducting proactive preventative engagements.

On 13 and 14 October 2021, Australia participated in the inaugural International Counter Ransomware Initiative Summit, hosted by the US. The Counter Ransomware Initiative seeks to enhance diplomatic efforts and international cooperation to combat the growing threat of ransomware. Australia leads the Initiative's Disruption Working Group, which has 27 nations as members. The Disruption Working Group is focussed on building individual and collective capacity for members to more effectively disrupt the threat of ransomware. Australia also participates in the Diplomacy, Resilience and Countering-Illicit Financing Working Groups.

In July 2021, ransomware actors targeted a vulnerability in software used by Kaseya (an IT solutions developer for managed service providers and enterprise clients). With more than a million systems affected and with the actors asking for a $70 million ransomware payment, many companies were affected. One notable example was the Swedish supermarket chain Coop, which closed down its 800 stores for a week, leaving some small villages without any supermarket alternatives.

Mobile malware

The COVID-19 pandemic has driven a sizable uptick in mobile device usage, creating a larger population of users for cybercriminals to target. This has been reflected in the last 12 months by an increase in smartphone malware. The majority of mobile malware is used to steal usernames and passwords for email or bank accounts, but many forms are also equipped with invasive snooping capabilities to record audio and video, track location, and wipe user content and data.

Since August 2021, many Australians have received scam text messages about missed calls, voicemails, deliveries and photo uploads carrying a malicious link that will download Flubot malware if clicked. Flubot malware enables cybercriminals to steal banking, contact, and personal information from an infected device.

Mobile device vulnerabilities have been exacerbated by the increase in remote work. Cybercriminals have also begun targeting Mobile Device Management Systems, which if successfully compromised, could enable hacker to access corporate systems.

Supply chain compromise

Malicious actors increasingly view the supply chain – including software, services and entities connected to businesses – as a priority target and vector for compromise. Targeting one weaker element of the supply chain can afford 'backdoor' access to a priority target, potentially providing system-wide access.

Modern supply chains – both digital and physical – are often expansive and complex ecosystems. Despite their sophistication, at their core supply chairs rely on trust to operate effectively.

Malicious cyber actors view supply chains as attractive targets for exploitation, as once access is obtained a cybercriminal can exploit these pre-existing relationships to attack a wide range of unsuspecting targets. Supply chain complexity significantly increases both the costs of defensive measures and the ability of cybercriminals to obtain a significant return.

In December 2020, Mandiant publicly announced a 'highly skilled actor' was conducting a global intrusion campaign enabled by the compromise of the SolarWinds Orion platform software. The compromise meant organisations running SolarWinds Orion platform software may have inadvertently installed malicious additions through normal update processes, and potentially provided actors with the ability to access users' systems. Following detection of the compromise and the quick release of advice and software patches, organisations were able to identify vulnerable versions of the Orion platform and remediate the vulnerability. SolarWinds engagement with ASD during this incident informed ASD's understanding of the potential impact to Australian organisations and its advice to Australians to protect their software and networks and enhance Australia's overall cyber security resilience.

Continued vulnerability exploitation

Cybercriminals and state actors continuously seek out software vulnerabilities. Once identified, they can create exploitation kits and then utilise tools such as automated scanners and bots to locate vulnerable systems for subsequent targeting.

Critical vulnerabilities such as Log4j are creating economies of scale for attackers, whereby malicious actors can weaponise vulnerabilities at great speed, allowing them to engage widespread exploitation.

Malicious actors are also becoming more efficient at exploiting zero-day vulnerabilities. In 2021, the average gap between time and the first known exploitation fell from 42 days to just 12 days.[7] The number of zero-days identified and exploited has also increased significantly, likely driven by greater detection and disclosure efforts, but also the rise of commercial vendors selling access to these vulnerabilities.

Growing Network Complexity

Global networks will continue grow in complexity and become more difficult to defend, with new and emerging technologies transforming the threat environment, as malicious cyber actors look to capitalise on old and new methods alike with the intent to exploit large numbers of victims. The headlining global cyber security events of 2020 and 2021 – such as the SolarWinds Orion supply chain compromises, the exploitation of on-premises Microsoft Exchange server vulnerabilities, and the Colonial Pipeline incident where ransomware actors significantly impacted distribution of fuel to customers on the United States' east coast – are now the new norm. Security of supply chains will remain imperative as technical vulnerabilities continue to emerge and Australia will experience more major financially motivated cyber incidents, some of which could disrupt critical services and infrastructure.

Rapid adaptation to vulnerabilities

Globally, COVID-19 themed scams occurred during the height of the pandemic. Malicious cyber actors targeted individuals and Australian organisations with COVID-19 related scams and phishing emails. This activity included the compromise of email servers belonging to health sector entities in Australia, which were then used to distribute COVID-19 phishing emails in an attempt to deploy malicious software, including ransomware, or to gain access to other targeted organisations.

Australia continues to see cybercriminals and state-based actors rapidly exploiting vulnerabilities, with the Log4j vulnerability a notable example in the 2021-22 financial year. In 2021, ASD continued to observe malicious cyber actors rapidly exploiting these vulnerabilities at scale, including against targets in Australia.

Over 2021-2022, Australian networks also suffered collateral impacts from widespread espionage campaigns where various actors sought to rapidly and indiscriminately exploit newly publicised vulnerabilities in Microsoft Exchange and Log4j, amongst others. These campaigns are becoming an increasingly regular part of the cyber security landscape.

Timely patching of critical vulnerabilities, and organisations configuring their networks and computers to minimise the impact of running malicious software, remain effective in protecting against these types of threats.

The substantial shift to remote working 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.

7 Analysing the Attack Landscape: Rapid7's 2021 Vulnerability Intelligence Report | Rapid7 Blog

Recommendations for Focus over the Next Year

The Committee will continue to provide advice on new and emerging cyber security issues and guide the effective implementation of the Strategy. The dynamic nature of the digital threat environment means that government responses to cyber threats need to be flexible and adapt to the changing landscape.

Based on the progress made to date on the implementation of the Strategy and in response to recent developments within the threat environment, the Committee recommends the following areas for particular focus over the next 12 months:

- Cyber security as a government priority and hardening government systems
- Improved evaluation and measurement
- Workplace readiness
- Protection and uplift of critical infrastructure and systems of national significance with strong industry consultation
- Cyber security skills
- Supporting SMEs
- Best Practice Regulations Taskforce
- Ransomware
- Threat information sharing
- Cryptocurrency.

Cyber security as a government priority and hardening government systems

The Committee welcomes the appointment of Australia's first dedicated Minister for Cyber Security and the establishment of the Cyber Security Coordinator at Home Affairs. The creation of these roles are important for the Government's focus on streamlining responsibilities and oversight of cyber security matters for Australia.

The Committee emphasises the continued importance of cyber security in the delivery of essential services to, and protection of, everyday Australians.

While some progress has been made on the Hardening Government IT program, it is important that government is a cyber security exemplar. The Committee strongly encourages the acceleration of this work.

Given the number of initiatives under the Strategy targeted at industry, both critical infrastructure and more broadly, it is important for the Government to take a strong leadership position in relation to hardening its own systems. Industry support will be harder to enlist if Government is not seen to be lifting its own defences at the same rate it is expecting businesses to.

Related to this is improving cyber security capabilities at the state and territory levels, and consideration needs to be given to how this should be undertaken to ensure consistent and holistic coverage across Australian governments.

Improved evaluation and measurement

It is critical that the government develop and implement an empirical, data-driven evaluation and measurement system.

The government has established an approach to program-level evaluations. However, insufficient progress has been made in developing this strategic evaluation framework.

This needs to include an overall integrated governance framework to monitor and manage the implementation progress of the many initiatives in the Strategy.

It is critical that this is also supported by a more ubiquitous and integrated empirical fact base of Australia's cyber maturity be established to measure the effectiveness of the initiatives being implemented under the Strategy, and to enhance future policy decisions at all levels of government.

This should include consideration of the development of a Cyber Security Maturity Index.

Workplace readiness

The COVID-19 pandemic forced many businesses and organisations to move to remote and hybrid working models. This has fundamentally changed the way Australians work.

The Committee remains of the view that businesses need to ensure they have the right defences in place to protect the workplace of the future, especially as Australia adopts more hybrid ways of working on a more permanent basis.

To assist with this effort, in November 2021 the Committee released a second thought piece outlining cyber security considerations for hybrid working in Australia. The Committee believes SMEs in particular need further assistance with ensuring they can remain safe and successful when operating a hybrid workforce, and that this should remain a focus for Government going forward.

Protection and uplift of critical infrastructure and systems of national significance (CI SONs) with strong industry consultation

The Committee encourages Government to continue to raise awareness to industry on the amended SOCI Act and provide the necessary direction and support to the critical infrastructure community.

The changes to SOCI Act under the CI-SONs initiatives of the Strategy have profound and far reaching implications for many operators of critical infrastructure. The telecommunication and financial services sectors already have considerable experience in adopting and complying with similar regulatory regimes under the Telecommunications Sector Security Reforms (TSSR) and the Australian Prudential Regulation Authority's Prudential Standard CPS 234. However, for other sectors identified under CI-SONs, these are new obligations. It is therefore crucial that the process of regulation development at the sector level allows for extensive industry consultation.

The Government should also extend the TISN to be more representative of the new expanded Australian critical infrastructure sectors and support businesses to align with the SOCI Act reforms. Uplifting cyber security arrangements are interwoven with each of these programs.

Cyber security skills

The Committee encourages Government to continue to involve industry in government-led cyber security initiatives, particularly those that focus on the skilled cyber workforce.

Cyber security skills are critical to ensuring we can effectively secure Australia's digital economy. The Committee believe Government should increase its focus on building the pipeline of entry level and industry roles in cyber through its leadership.

Government should also look carefully at lessons learnt from current skills and workforce participation activities, such as the Australian Defence Force Cyber Gap Program, and amplify those activities which have led to a surge in number of applicants and higher participation rates.

The Government can also play a direct role to encourage and assist Australian educational institutions to build more basic cyber skills into a broader range of curriculums in software engineering, robotics and other tertiaries. Deep cyber specialists are important, but Australia also needs to better equip a broader range of technologists.

Supporting SMEs

As the Government explores opportunities for uplifting Australia's cyber security in the evolving threat landscape, it is critical that consideration is given to ensuring any advice, assistance or regulatory measures are not only effective, but are also simple to use. This should focus on SMEs in particular, which have historically had difficulties with cyber uplift.

The Committee encourages the Government to provide further assistance targeted at SMEs to raise their awareness of best practice cyber behaviours, to help them understand and meet their regulatory requirements, and to support them with transitioning to and operating a hybrid workforce.

Best Practice Regulations Taskforce

During 2021, the Committee provided advice on options for regulatory reforms and voluntary incentives to strengthen the cyber security of Australia's digital economy as part of the Strengthening Australia's Cyber Security Regulations and Incentives 2021 discussion paper.

The Committee emphasised the importance of clarifying the responsibilities and duties of companies which are not captured under new critical infrastructure legislation, in relation to cyber security.

The Committee considers that clarifying the responsibilities and duties of boards, beyond those captured under the critical infrastructure legislation, and their directors in relation to cyber security through voluntary governance standards for cyber best practice is a critical and urgent next step in this work.

Consultation with industry was commenced more than a year ago, with submissions due in September 2021. Industry is yet to receive any feedback from Government on its conclusions from this important work.

Ransomware

Ransomware continues to be one of the most prominent forms of malicious cyber activity today. The Committee released its first thought-piece *Locked Out: Tackling Australia's ransomware threat* in March 2021 to build awareness for all Australians and their businesses on the ransomware threat landscape.

The Committee welcomed the release of Australia's Ransomware Action Plan, which articulates that Australia does not condone the payment of ransoms to cybercriminals.

The Committee looks forward to hearing updates on the reforms to modernise legislation to ensure that cybercriminals are held to account for their actions, and progress made to consult on and develop the mandatory ransomware incident reporting regime.

Threat information sharing

Threat sharing is key to keeping on top of malicious activity. The Committee welcomes the development of the ASD's CTIS platform to boost intelligence sharing across industry and government.

The CTIS platform will provide a significant boost to intelligence sharing across industry and government. Now that the platform has exited the pilot stage, accelerating its final refinements and onboarding new organisations should be a priority.

The Committee encourages the Government to continually strengthen information sharing between government and industry, particularly on threats. Threat sharing is essential to threat blocking and network resilience.

The Committee also continues to recognise the value of the ASD's JCSCs and recommends the Government continue to focus on elevating their role as they play a key point of alignment and cooperation between government, states and territories, and industry. While a significant investment has been made in transforming JCSCs, it is important that government continues to realise their full potential and ensure their effectiveness is measured.

The JCSCs were a capability recommended under the 2016 Cyber Security Strategy, and their utility in facilitating collaboration and threat sharing further recognised under the current Strategy. Given the significant role they can play in improving Australia's cyber defences, progress on their development and maturity should be accelerated.

Cryptocurrency

Cryptocurrency was the subject of the Committee's third public thought-piece. Cryptocurrency is often at the epicentre of cybercrime and is favoured by criminal groups to facilitate online crime due to its anonymous nature. It is the currency of choice by criminals for ransomware payments.

There are also many positive use cases for cryptocurrency, and it is becoming increasingly institutionalised. Given the rapid growth in both the number of cryptocurrencies available and their value, the purpose of the thought-piece was to:

- stimulate conversation about the evolution of cryptocurrency, the technology that underpins it, and its cybersecurity considerations
- explore some of the components of cryptocurrency, supported by case studies
- provide guidance and recommendations on using cryptocurrency.

The thought-piece included several recommendations, particularly in relation to the strengthening of the regulation of DCEs. The Committee recommends these be prioritised by Government.

Other Considerations – a holistic approach to the integrity of our digital platforms

Technology underpins Australia's most important services and systems. While technology presents significant opportunities, Australia must stay ahead of the risks.

Almost all technologies have security implications of some kind. For example, smart cities capture a suite of technologies such as data, 5G and future connectivity, Internet of Things devices and Artificial Intelligence. These elements converge to a new multifaceted challenge.

While the Committee's main focus is on building cyber security defences, the Government should take a holistic and inclusive approach to the suite of digital security challenges. This includes cyber security as well as access to and security of critical technologies, and how they interrelate.

Critical technologies

The Committee supports the Blueprint and Action Plan for Critical Technologies. Critical technologies are current and emerging technologies with the capacity to significantly enhance or pose risk to the national interest. Australia's ability to harness the opportunities created by critical technologies has significant impacts on national economic success, security, and social cohesion.

Australia has identified 23 critical technologies, including protective cyber security, telecommunications, quantum computing, machine learning and advanced robotics.

Access to - and the resilience of - technology systems is of national importance. However, geopolitics and global economics play a major role in the supply chain of the critical technologies on which Australia's future depends. Many critical technologies rely on common key components. For example, most telecommunications networks globally rely on 5G radio technologies, and all computers rely on semiconductors. The supply of both has become incredibly concentrated and politically influenced.

To protect national digital infrastructure, government policies on cyber security and critical infrastructure need to be aligned.

The Committee also recommends that focus should be given to uplifting quantum encryption. In this regard, the Committee welcomed the $111 million government investment to secure Australia's quantum future, supporting the commercialisation, adoption and use of this new technology to create jobs, support Australian businesses and keep Australians safe.

International collaboration

Securing the integrity of our digital platforms will also require the Government to continue to collaborate internationally. The Committee emphasises the importance of Australia's International Cyber Security and Critical Technologies Strategy under the Department of Foreign Affairs and Trade. Having a seat at the table for global standards discussions is crucially important to Australia.

The Committee recognises that Australia continues to work closely with international like-minded nations to improve cyber defences. Most recently, the Quad Senior Cyber Group is working to adopt and implement shared cyber standards, develop secure software, build workforce and talent, and promote the scalability and cyber security of secure and trustworthy digital infrastructure.

The Committee supports collaboration and information sharing in relation to government attribution to malicious cyber activity, which includes the recent joint attributions and condemnation of the malicious cyber activity by Russia in the lead up to the Ukraine invasion. This was a powerful example of international cooperation and political will to call out activity which has the potential to undermine global economic growth, national security and international stability. Australia should continue to publicly attribute cyber incidents when it is in our interests to do so.

In summary, cyber security is just one part of the matrix of policy initiatives the Government needs to keep in sharp focus to protect the integrity of Australia's digital platforms.

Given the impact of the COVID-19 pandemic and the subsequent unprecedented adoption of digital platforms and technological innovation, Australia must be vigilant of the underlying technology on which Australians depend.

Australia's technologies need a level of proportionate risk management and in built security requirements (including cyber security). These requirements will balance the wide-ranging applications and benefits for Australia's society and economic development.

The Government's approach to digital technologies should consider how security is built into the next phase of computing and internet infrastructure, where the issues of technology and cyber converge.

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 more than 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

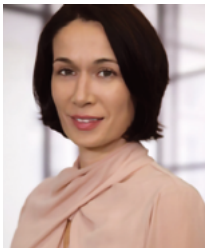
Ms Reid is the Chair of AUCloud and Co-Founder of Icon Group, a provider of integrated cancer care services with operations in Australia, Singapore, New Zealand and China where she served as Digital Advisor to the Icon Group board until July 2020. She also Co-Founded Australia's Epic Pharmacy Group. 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 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.

Mr Chris Deeble AO CSC

Mr Deeble is the former 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.



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 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 David Tudehope

David is Chief Executive and co-founder of Macquarie Telecom Group and has been a director since 16 July 1992. 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 members of the Australian Government's B20 Leadership Group. David holds a Bachelor of Commerce degree at the University of NSW. In 2018, David was named Australian Communications Ambassador at the 12th Annual ACOMM Awards. In 2020, David was named CEO of the Year at the World Communications Award in London.

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.

Appendix B:
Australia's 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.	– Amendments to the *Security of Critical Infrastructure Act 2018* that came into effect in December 2021 and April 2022 have strengthened Australia's ability to manage and respond to security risks across 11 critical infrastructure sectors. The *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* came into force in April 2022. – These reforms are part of a range of measures the Australian Government is putting in place to strengthen Australia's ability to manage and respond to security risks across critical infrastructure sectors.

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.	– In August 2021, ASD's National Exercise Program (NEP) delivered AquaEx, a major exercise for Australia's urban water and wastewater sector and government agencies. In addition, NEP delivered exercises with individual critical infrastructure organisations, and provided exercise management training workshops to specific entities to help them improve their cyber incident response capabilities. – In December 2020, the former Government in cooperation with states and territories reviewed the CIMA policy through the National Cyber Security Committee (NCSC). – The NCSC Policy Subcommittee developed recommendations to update the CIMA policy and implementation of the review recommendations is underway. – The CIMA was exercised with members of the National Cyber Security Committee in May 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 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 cybercrime, including on the dark web. The Australian Government will extend and expand the ASD'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 cyber criminals. This builds on the Australian Government's election commitment to counter foreign cyber criminals. 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 ASD identify and disrupt more cybercrime targets. – Agencies have the authorities they need to discover, target, investigate and disrupt cybercrime and cyber-enabled crime, including high volume cybercrimes affecting the Australian community. – More responses to online crimes are coordinated between the Australian Government, states and territories	– *The Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* commenced on 4 September 2021. – The National Plan to Combat Cybercrime launched on 21 March 2022. – Launch of the National Cybercrime Capability Fund to uplift law enforcement capability to combat cybercrime. – The AFP's Joint Policing Cybercrime Coordination Centre (JPC3) launched on 21 March 2022, bringing together capabilities from across State and Territory law enforcement agencies, Commonwealth government agencies and key private sector partners from the Australian business community, to coordinate Australia's policing response to high volume, high harm cybercrime. – During the 2021-22 financial year ASD issued almost 62,000 adverse website takedown notifications. – ASD has supported law enforcement partners, and used its offensive cyber capabilities to generate effects to undermine and disrupt cyber criminals 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. Government agencies will also put a renewed focus on policies and procedures to manage cyber security risks.	**Allocated:** $50.0 million.	– Centralisation of Australian Government IT networks makes it easier to defend against malicious activity.	– As at 30 June 2022, three pilot hubs (Defence, Home Affairs and Services Australia) have been stood up and commenced on-boarding of the six client entities involved in the pilot. In the 2022-23 Budget, the Australian Taxation Office was given authority and funding to commence a fourth Cyber Hub. – Cyber Hubs are delivering core services in a live production environment and are already demonstrating improvements in client entities' cyber security maturity. – The ASD is providing advice and assistance to government entities, and supporting prioritised entities through the Cyber Maturity Measurement Program (CMMP). In 2021, the ASD delivered the CMMP to nine government entities and also delivered the ASD Cyber Security Uplift Services for government to 21 entities. – During the remainder of 2022, the ASD will undertake CMMP assessments with each of the Cyber Hub providers. – CMMP will continue through 2022 and 2023 to finalise the Hubs agencies.

Initiative	Description	Funding	Measuring Success	Implementation progress
5. Improve threat information sharing	The Australian Government will, through the ASD, deliver a new partner portal coupled with a multi-directional threat-sharing platform. The Australian Government will enhance the cyber security of Australian universities by engaging RMIT to pilot a threat intelligence-sharing network, sector-specific threat modelling materials and supporting six national cyber security forum meetings across FY20-21 to FY21 22. The former Government, through Home Affairs, is extending and enhancing the Trusted Information Sharing Network (TISN) - industry and all levels of government's primary way of engaging to enhance the security and resilience of critical infrastructure. The TISN is where members of the critical infrastructure community collaborate, to strengthen the resilience of their organisations in the face of all-hazards, including cyber security.	**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 actionable cyber threat intelligence to defend and counter cyber threats at near real time.	– In November 2021, ASD launched the Cyber Threat Intelligence Sharing (CTIS) platform. At the end of the financial year, CTIS had more than 30 partners using the platform. Of these partners, half are sharing threat information bidirectionally. More than 34,000 IOCs were shared over the period. – The RMIT pilot is now focused on the development of threat assessment and modelling materials for the university sector. – Work has progressed on the development of best practice guides, models and training modules to support universities (drawing from the Essential 8, AISM). All products are due end of 2022. – The Critical Infrastructure Resilience Strategy 2022 has been drafted, pending finalisation. The Strategy recognises TISN as a key pillar to uplifting security and resilience. – The TISN has been expanded to include additional energy, resource and data sector groups. Existing groups being revitalised include health, transport, and food and grocery. A collaborative platform is also being rolled out to enhance national threat sharing and collaboration.

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 Cyber and Critical Technology International Engagement Strategy was released. – In July 2021, Australia made a voluntary national contribution to the UN Group of Governmental Experts on Advancing responsible state behaviour in cyberspace in the context of international security (GGE) official compendium on how international law applies to the use of information and communications technologies by States. – To support international law and norms of responsible state behaviours, the Australian Government has continued its policy of public attribution. On 19 July 2021, the former Australian Government joined international partners in expressing serious concerns about malicious cyber activities by China's Ministry of State Security in regards to exploited vulnerabilities in the Microsoft Exchange software. In February 2021, the former Australian Government joined international partners in publicly attributing the distributed denial of service (DDoS) attacks against the Ukrainian banking sector on 15 and 16 February 2022 to the Russian Main Intelligence Directorate (GRU).

Initiative	Description	Funding	Measuring Success	Implementation progress
7. Strengthen cyber security partnerships	The Australian Government will expand the ASD's JCSC program. A broader range of ASD 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 has established a Home Affairs national outreach program with officers embedded in each JCSC to amplify government's approach to uplifting Australia's cyber security awareness and capability across the economy. The Outreach Officers provide entities, particularly critical infrastructure entities and entities in the supply chain, with advice and assistance on where to access information to improve their cyber hygiene with a view to uplifting their security and resilience, with a key focus on cyber hygiene.	**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.	– In the 2021-22 financial year, JCSCs hosted more than 370 events. – Outreach services at 'virtual offices' in Darwin and Hobart are now open. – ASD has expanded the Partnership Program, with the number of Network Partners increasing by more than 30% over the 2021-22 financial year. – Home Affairs Outreach Officers are embedded in the JCSC regional offices in Perth, Brisbane, Melbourne and Adelaide, and recruiting officers in Sydney, Darwin and Hobart.

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. Entities who fall within the asset classes defined in the SOCI Act have cyber security reporting and preparedness obligations place on them. Either through SOCI or via another regulatory / commercial contract construct. Consultation for obligations for businesses that are not critical infrastructure 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.	– On 27 August 2021, consultation on options for regulatory reforms and voluntary incentives to strengthen cyber security across the Australian digital economy, including in the areas of smart devices concluded. These reforms complement the new critical infrastructure reforms.

Initiative	Description	Funding	Measuring Success	Implementation progress
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. – In November 2021, the Blueprint and Action Plan for Critical Technologies in the national interest was published. – The ASD's research program addresses a number of security challenges in the next generation of technologies used by Australians.

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. ASD has received 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 ASD to understand and respond to cyber threats on a national scale.	**Vulnerability 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.	– On 2 December 2021 the *Security Legislation Amendment (Critical Infrastructure) Act 2021* came into force. Key features of the *Security Legislation Amendment (Critical Infrastructure) Act 2021* include Enhanced Cyber Security Obligations, and Government Assistance to relevant entities for critical infrastructure assets in response to cyber-attacks. – Mandatory reporting of cyber security incidents that reach certain thresholds came into effect on 8 April 2022, following extensive consultation with industry. Following a three month period to allow for industry to prepare for this new obligation, from 8 July 2022 the obligation became mandatory for certain asset critical infrastructure classes. **Note:** As of 7 July2022 Critical telecommunications assets have the same obligation under the *Telecommunications Act 1997* – On 2 April 2022, the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* came into force.

Initiative	Description	Funding	Measuring Success	Implementation progress
10. Improve baseline security for critical infrastructure				– The Minister for Home Affairs now has the power to 'switch on' the risk management program (RMP) for specified critical infrastructure asset classes and require those entities to develop and implement a risk management program to mitigate or eliminate material risks to their business. Rules under the RMP are proposed to include compliance with a specified cyber security standard or equivalent. – ASD has also made enhancements to ReportCyber to facilitate improved incident reporting and development of a national threat picture. – ASD began a pilot critical infrastructure uplift program focussed on identifying vulnerabilities and providing advice on bolstering cyber resilience in August 2021. As of the end of June 2022, two uplifts have been completed under the pilot program.

Initiative	Description	Funding	Measuring Success	Implementation progress
11. Uplift the cyber security of SMEs	The Australian Government established 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. The Home Affairs Cyber and Infrastructure Security Outreach officers work with SMEs, with a particular focus on critical infrastructure entities, or those entities that sit within the supply chain of critical infrastructure entities, providing them with advice and assistance on where to access information to improve their cyber hygiene with a view to uplifting their cyber security and resilience.	**Allocated:** $8.3 million.	– An increasing number of small businesses have improved their cyber security practices.	– Cyber Security Connect and Protect Program launched October 2020. 14 successful applicants were announced in April 2021. Projects were completed in March 2022. – Evaluation of the Cyber Security Connect and Protect Program is in progress, with a completion target of the end of 2022. This evaluation will identify the most effective approaches to support future efforts to uplift SME cyber security. – The ASD has released a suite of small business guidance, including the *Small Business Cyber Security Guide, the Cyber Security Prevention and Emergency Response Guides, Step-by-Step Guides and Quick Wins*.
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 former 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. – In mid-2021, the Best Practice Regulation Taskforce undertook public consultation to consider whether additional action on Internet of Things security is needed. The Government is currently considering next steps.

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 ASD 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.	**Cyber Security Skills Partnership Innovation Fund** **Allocated:** $70.3 million. **ASD 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:** $41.26 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 2 of the Cyber Security Skills Partnership Innovation Fund was announced on 25 October 2021 and applications closed 6 December 2021. Round 2 outcomes will be considered by the Government. – ASD launched the pilot of the Australian Women in Security Mentoring Program in May 2021 with 110 participants. The Program will be launched publicly in August 2022. – ASD Women in Cyber program also delivered technical training scholarships for women; sponsorship of career pathway, leadership and CISO training for women cadets and professionals; sponsorship of CyberTaipan 2022, Go Girl, Go For IT 2022 career fair, Girls Programming Network, and GROK Academy cyber challenges; and ongoing delivery of ASD's CyberEXP. – The targeted update of ANZSCO to include security occupations was released in November 2021. – ADF Cyber Gap Year Pilot Program commenced in July 2020 with 47 participants, with 46 graduated in June 2021. Applications for Intake 2 opened in September 2021, with 1267 applications received for 300 positions; 282 applicants accepted the offer. Intake 3 will commence in January 2023.

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:** $12.5 million.	– More known malicious threats are prevented from reaching Australians.	– As of June 2022, more than 75,000 host-based sensors were deployed on government agencies networks to detect malicious activity and cyber threats. – On 25 November 2021, the *Telecommunications (Interception and Access) Amendment (2021 Measures No. 1) Regulations 2021* were made, giving industry confidence to deploy tools to block malicious SMS scams and protect their systems.

Initiative	Description	Funding	Measuring Success	Implementation progress
Actions by the community				
15. Access guidance and information on cyber security	The community needs to act on best practice advice from the ASD 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 ASD 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. The Cyber and Infrastructure Security Centre is developing guidance material in consultation with industry, including for new cyber security incident reporting, asset registration and the risk management program obligation.	**Cyber Security Awareness Raising campaigns** **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.	– The Home Affairs-led cyber security awareness raising campaign 'Beat cybercrime in your down time' ran between October 2021 and December 2021. It encouraged Australians to re-evaluate their cyber risk, and take control of their own cyber security. – In the 2021/22 financial year, the Act Now, Stay Secure advertising campaign delivered over 57 million online ads to Australians though social media, video and search and reached over 6.2 million Australians through broadcast radio advertising. – The independent evaluation of the campaigns indicated they performed very strongly and drove substantial increased traffic to cyber.gov.au where users followed the simple steps to increase their cyber security resilience. – In October 2021, ASD released online learning resources on cyber.gov.au to support Australian small businesses, Australian individuals and families. – Cyber security threat and advisory information is being amplified through the TISN and on the www.CISC.gov.au website to target critical infrastructure stakeholders. – Learn Hub was launched in October 2021 and had attracted more than 30,000 users by June 2022.

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 ASD expanding its assistance to the SMEs and the community. The Australian Government will also bolster services to victims of identity and cybercrime. All critical infrastructure entities should access resources to understand the obligations placed on them by amendments to the SOCI Act - www.cisc.gov.au	**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 ASD's expanded 24/7 helpdesk. – Increased understanding of the impacts of cybercrime on the community.	– On 25 January 2021, Home Affairs signed a contract with IDCARE for specialist identity and cybercrime support services over four years from 2020-21 financial year. The funding was allocated to bolster services to victims of identity and cybercrime. Up to 30 June 2022, the organisation has provided more than 30,913 case management services and 924 Cyber First-Aid services. – On 25 November 2021, the new 1300 Cyber Hotline was formally launched. The Cyber Hotline has substantially enhanced operator coverage, services and support for callers. – Between July and November 2021, the hotline recorded an average of almost 2000 calls per month. Following the expansion on 25 November 2021, this monthly average rose to approximately 2,200 calls by end of the 2021-22 financial year.

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.	
Other commitments				
18. Strengthen Australia's national system of identity settings	The Australian Government will work with states and territories to strengthen arrangements for issuing and managing identity documents, maintain strong privacy safeguards, and further bolster our defences against identity and cybercrime.	**Allocated:** $2.8 million to be absorbed from within the 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. – Phase one of the strengthening national identity initiative, Review of the National Identity Proofing Guidelines, has been completed.
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.		– Australia's *Critical Technology Supply Chain Principles* (The Principles) were released. – Home Affairs has released a baseline survey in early 2022 to gain insight and understanding on how organisations currently consider the security of their technology supply chains. – A review of the Principles will be conducted 12 months after their release.

Appendix C:
Overview of Evaluation Results of *Australia's Cyber Security Strategy 2020**

Progress to date on the Strategy's programs and deliverables

Key factors of success

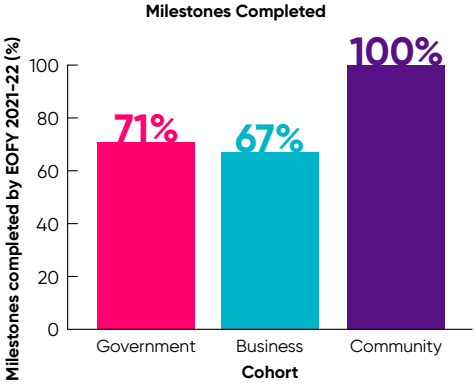
Programs reported strong engagement as the key to their success. For example, the Critical Technology Supply Chain Principles engaged with industry to ensure changes would take into account the views of those affected, increasing stakeholder buy-in. Other programs such as the Questacon Cyber Program or the ASD's Education and Skills Programs mobilised targeted engagement and educational programs to grow the cyber skilled workforce of the future.

Some other key factors reported by program leads included innovation and the uplifting of technological capabilities, with programs assisting target cohorts to uplift their cyber security capability while also contending with the disruptive effects of the COVID-19 pandemic. Additionally, many programs led the development of new best practice guidelines, regulatory changes and legislative amendments to uplift the cyber security of Australia's critical infrastructure, businesses and Australian communities.

Milestone completion

Programs across the Strategy's Government, Business and Community cohorts reported that 73 per cent of their milestones have been completed to date. Under the Community cohort, all programs have achieved their milestones and are considered complete, with the Business cohort having the most milestones remaining out of the three groups.

The Strategy has delivered eleven programs and is on track for an additional twelve programs to complete all their milestones by end of 2022-23, with another five due for completion by end of 2023-24.



100%
OF PROGRAMS
UNDER THE STRATEGY HAVE SUPPORTED IMPROVEMENT OUTCOMES FOR THEIR TARGET COHORT

87%
OF PROGRAMS
UNDER THE STRATEGY HAVE CONTRIBUTED POSITIVELY TO ITS STRATEGIC INTENT

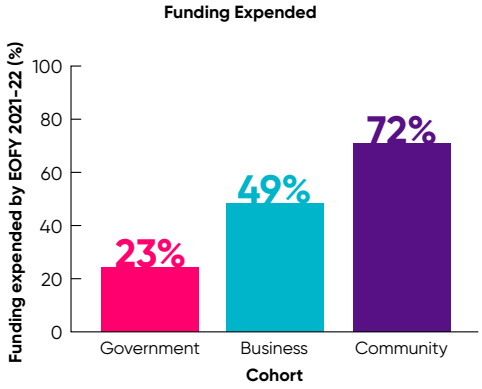
Outcomes measured

The most common outcome (49 per cent) used to measure success was stakeholder accessibility and uptake, as many programs under the Strategy sought to improve their target cohort's cyber capabilities and produce assistive resources. The next most frequent outcomes measured were reducing harms to Australians, influencing better cyber behaviours in business and community, and passing legislation to reform how law enforcement and critical infrastructure entities deal with cyber.

Value for money

Of the funding allocated to programs under the Strategy, 36 per cent has been expended to date. Most of these programs have expended over half of their allocated funding as of 30 June 2022, and the expenditure of sensitive programs are on track with the work accomplished thus far. Government programs have the lowest proportion of funding expended primarily due to the longer implementation timeframes of initiatives under this cohort.

Return on investment was often measured through the quality and quantity of stakeholder engagements or cost-benefit analysis exercises.



72% **OF PROGRAMS** UNDER THE STRATEGY HAVE ACHIEVED THEIR CRITICAL OUTCOMES, ALL OUTCOMES OR HAVE EXCEEDED EXPECTATIONS

100% **OF PROGRAMS** UNDER THE STRATEGY HAVE EVIDENCE TO SUPPORT VALUE FOR MONEY

Opportunities for improvement

40 per cent of programs did not identify opportunities for improvement, broadly indicating that programs were effective. However, there are four main opportunities to improve Australia's cyber approach:

1. Expand or add targeted engagement and education campaigns to support uplift in baseline technological capabilities across government, business and community.
2. Create more avenues for industry and community to engage with programs.
3. Enhance whole-of-government and interdepartmental coordination of cyber security programs under the Strategy.
4. Provide additional staff resourcing and funding to existing cyber programs to help them maximise the impacts of their work.

* Captures data provided by 43 out of 47 reporting Strategy programs in the Government, Business and Community cohorts, not including sensitive programs. Totals may vary due to rounding.