AUSTRALIA'S
CYBER SECURITY STRATEGY

Enabling innovation, growth & prosperity

Australian Government

TABLE OF CONTENTS

PRIME MINISTER'S FOREWORD

This Cyber Security Strategy sets out my Government's philosophy and program for meeting the dual challenges of the digital age—advancing and protecting our interests online.

The maintenance of our security online and the protection of freedom online are not only compatible but reinforce each other. A secure cyberspace provides trust and confidence for individuals, business and the public sector to share ideas, collaborate and innovate.

The Internet is transforming how we socialise and do business in ways its founders could not have imagined. It is changing how we are entertained and informed, affecting almost every aspect of our lives.

The need for an open, free and secure Internet goes far beyond economics.

It is important for ensuring public and financial accountability and strengthening democratic institutions. It underpins freedom of expression and reinforces safe and vibrant communities.

If we are to fully realise the social, economic and strategic benefits of being online, we must ensure the administration of the Internet continues to be governed by those who use it—not dominated by governments.

Equally, cyberspace cannot be allowed to become a lawless domain. Both Government and the private sector have vital roles to play. While governments can take the lead in facilitating innovation and providing security, businesses need to ensure their cyber security practices are robust and up to date.

Australia and Australians are targets for malicious actors—including serious and organised criminal syndicates and foreign adversaries—who are all using cyberspace to further their aims and attack our interests. The scale and reach of malicious cyber activity affecting Australian public and private sector organisations and individuals is unprecedented. The rate of compromise is increasing and the methods used by malicious actors are rapidly evolving.

The Australian Government has a duty to protect our nation from cyber attack and to ensure that we can defend our interests in cyberspace. We must safeguard against criminality, espionage, sabotage and unfair competition online.

Australia and its allies will work together internationally to promote norms of behaviour that are consistent with a free, open and secure Internet. These norms include that states should not knowingly conduct or support cyber-enabled intellectual property theft for commercial advantage. We need to do this while redoubling our efforts to counter

the spread of propaganda online which incites extremist and terrorist violence.

As the Snowden disclosures demonstrate, often the most damaging risk to government or business online security is not 'malware' but 'warmware'; the ability of a trusted insider to cause massive disruption to a network or to use legitimate access to obtain classified material and then illegally disclose it.

Technical solutions are important but cultural change will be most effective in mitigating this form of cyber attack.

As businesses and governments we must better educate and empower our employees to use sound practices online. This Strategy seeks to promote an improved institutional cyber culture and raise awareness of cyber practice across government and business to enable all Australians to be secure online.

The Strategy complements the key elements of my Government's Economic Plan—helping the transition to a new and more diverse economy which is fuelled by innovation, the opening of new markets and more investment in Australian enterprise. The cyber security industry is in its relative infancy but undergoing rapid growth. Australia is well placed to be a leader in cyber security. We can use technology as a means to manage the threats and risks that come with being online and interconnected—and to grow our true potential.

With the Innovation and Science Agenda and the Defence Industry Plan, this Strategy will help bring more Australian technologies to market, prepare our children for the jobs of the future by boosting science, technology, engineering and mathematics (STEM) participation and support and create innovative Australian companies.

Most importantly, this Strategy will play a key role in securing Australia in the 21st Century. It also represents a significant investment in cyber security. The Government will invest more than $230 million over four years to enhance Australia's cyber security capability and deliver new initiatives. This complements the significant investment in cyber security outlined in the 2016 Defence White Paper, boosting Defence cyber capabilities by up to $400 million over the next decade.

The Government will show leadership locally, regionally and globally. I will designate a Minister Assisting the Prime Minister on cyber security and appoint a Special Adviser on Cyber Security in my Department, the Government's lead on cyber security policy. The Minister for Foreign Affairs will also appoint Australia's first Cyber Ambassador and the Department of Defence will continue to lead the co-location of the Government's operational cyber security capabilities in the Australian Cyber Security Centre.

This new structure will ensure cyber security is given the attention it demands in an age where cyber opportunities and threats must be considered together and must be addressed proactively, not simply as a reaction to the inevitability of future cyber events. This Strategy will develop partnerships between the Australian public and private sectors, support home-grown cyber security capabilities and promote international cyber cooperation. We will change and adapt when needed to stay competitive and influential in the constantly changing technology landscape.

I look forward to working with governments both at home and abroad, the private sector and the community to strengthen trust online and together better realise Australia's digital potential.

The Hon Malcolm Turnbull MP
Prime Minister
21 April 2016

EXECUTIVE SUMMARY

Strong cyber security is a fundamental element of our growth and prosperity in a global economy. It is also vital for our national security. It requires partnership involving governments, the private sector and the community.

Being connected is now essential, creating new opportunities for innovation and growth for all Australians. To be competitive, businesses need to be online. But this also brings risks. Australia is increasingly a target for cybercrime and espionage. All of us—governments, businesses and individuals—need to work together to build resilience to cyber security threats and to make the most of opportunities online.

To grow, Australia needs to innovate and further diversify its economy—to access new markets and new forms of wealth creation. We must embrace disruptive technologies; those that have the potential to fundamentally change traditional business models and the way people live and work. They will open up new possibilities for agile businesses in ways as yet unimagined.

But the potential of digital technologies depends on the extent to which we can trust the Internet and cyberspace. Getting cyber security right will mean we capture more of the opportunities the connected world offers. It will also make Australia a preferred place to do business. This in turn will boost our national prosperity. We can also expand our cyber security businesses and export capability.

Australia's cyber security is built on a solid foundation. Our past investment has been strong. Recent Government initiatives such as the Australian Cyber Security Centre have lifted Government capabilities to a new level. Many of our larger businesses, particularly banks and telecommunications companies, have strong cyber security capabilities. Our future work will build on this platform.

We must also do more. If an organisation is connected to the Internet, it is vulnerable to compromise. As people and systems become ever more interconnected, the quantity and value of information held online has increased. So have efforts to steal and exploit that information, harming our economy, privacy and safety. Cyberspace, and the dynamic opportunities it offers, is under persistent threat.

Malicious cyber activity is a security challenge for all Australians. Australian organisations across the public and private sectors have been compromised by state-sponsored or non-state actors. Overseas, large multinational companies and government organisations have been targeted, losing substantial amounts of sensitive commercial and personal information or incurring major damage to their business and reputation.

To grow our cyber security capabilities to anticipate and respond to cyber threats, we must address our shortage of cyber security professionals. It is critical that we build our nation's stock of cyber security skills, which are becoming increasingly essential for life and work in our connected world.

Ultimately, to deal with all these challenges we must elevate cyber security as an issue of national importance. Leadership will be critical to achieving this goal.

The Australian Government will take a lead role and in partnership with others, promote action to protect our online security. Much of our digital infrastructure is owned by the private sector, so securing Australia's cyberspace must also be a shared responsibility. It will be important that businesses and the research community work with governments and other stakeholders to improve our cyber defences and create solutions to shared problems.

A STRATEGY TO SECURE OUR PROSPERITY IN A CONNECTED WORLD

The Government is committed to enabling innovation, growth and prosperity for all Australians through strong cyber security. This is in line with the Australian Government's broader National Innovation and Science Agenda to help to create a modern, dynamic, 21st Century economy for Australia.

This Strategy establishes five themes of action for Australia's cyber security over the next four years to 2020:

1. A national cyber partnership

2. Strong cyber defences

3. Global responsibility and influence

4. Growth and innovation

5. A cyber smart nation

Each theme is supported by actions the Government will take to improve our cyber security and ensure Australia can continue to grow and prosper today and to seize opportunities for tomorrow. Recognising that cyberspace is dynamic, the Strategy's initiatives will be reviewed and updated annually and the Strategy reviewed and updated every four years.

Some actions are already underway and will be ongoing. Others are new and will be co-designed with stakeholders from the private sector, research community and international partners. Many of these actions also rely on working with all Australians—because we all have a part to play in enhancing our security and confidence in Australia as a modern economy and trusted place to do business.

The ideas that underpin this Strategy were drawn from a classified Cyber Security Review led by the Department of the Prime Minister and Cabinet. The Department, through the new position of a Special Adviser on Cyber Security, will lead implementation of this Strategy for the Government, in its central responsibility for cyber security policy.

Ultimately, all of us—governments, businesses, communities and individuals—need to tackle cyber security threats to make the most of online opportunities. This Strategy charts a new way forward for Australia's cyber future, one that is creative, collaborative and adaptable.

A NATIONAL CYBER PARTNERSHIP

Together, the Australian Government and business leaders will jointly drive Australia's cyber security, **setting the strategic agenda** through annual Cyber Security meetings. Hosted by the Prime Minister and comprising leaders from business and the research community, the meetings will align the key initiatives in this Strategy and tackle emerging cyber security issues. A Minister Assisting the Prime Minister on cyber security will also underpin this effort.

We will **streamline the cyber security governance** for Commonwealth Government agencies and clearly identify lead responsibilities. Further, the Australian Cyber Security Centre will be relocated to a facility that allows the centre to grow and enables the Government and the private sector to work more effectively together.

We will also sponsor research to better understand the **costs of malicious cyber activity** to the Australian economy to ensure organisations have local information to inform their investment and risk management decisions for cyber security.

STRONG CYBER DEFENCES

Australia's networks and systems will be increasingly resilient to attack and hard to compromise. We will better **detect, deter and respond to cyber security threats** and better anticipate risks.

Australian governments and the private sector will work together to share more information, including from classified sources, exchanging information on threats and responses through joint cyber threat sharing centres in key capital cities and an online cyber threat sharing portal.

We will jointly exercise our response to be better prepared for cyber attacks. The Government will invest in agencies in the Australian Cyber Security Centre. We will increase the capacity of the national Computer Emergency Response Team (CERT) Australia to work with Australian businesses, in particular those providing national critical services. We will also improve the Australian Signals Directorate's ability to detect cyber security vulnerabilities. This will complement the investment in cyber capabilities being made through the 2016 Defence White Paper.

The Government will improve its capacity to tackle cybercrime by increasing the number of specialists conducting threat detection and awareness, technical analysis and forensic assessments of cybercrime in the Australian Crime Commission and the Australian Federal Police.

Australia will **raise the bar on cyber security performance**. Organisations in both the public and private sectors need to better understand cyber risks and have stronger cyber defences. Cyber security is too often viewed as simply an IT issue—it belongs at the centre of business strategy, for organisations across the public and private sectors. Governments, businesses and the research community will co-design national voluntary cyber security guidelines to promote good practice that all organisations can use. These will be based on world class strategies developed by the Australian Signals Directorate and aligned with international standards where possible. Voluntary cyber security governance 'health checks' will also help organisations understand their cyber security strengths and gaps.

GLOBAL RESPONSIBILITY AND INFLUENCE

Australia will work with its international partners to **champion an open, free and secure Internet**. We will work together to address cyber security threats and highlight the opportunities a free Internet presents for the global economy. This work will be enhanced through the appointment of a Cyber Ambassador who will identify opportunities for practical international cooperation and ensure Australia has a coordinated, consistent and influential voice on international cyber issues.

Australia supports a cyberspace in which states abide by international law and their behaviour is supported and reinforced by agreed norms—or standards for appropriate conduct—and practical confidence building measures that reduce the risk of conflict.

Most cybercrime targeting Australians originates overseas, so the Government will partner with international law enforcement, intelligence agencies and other computer emergency response teams. This will **build cyber capacity** to prevent and **shut down safe havens for cyber criminals**. Australia's capacity building assistance will also enable our international partners, particularly in the Indo-Pacific region, to develop their institutional capacity to tackle cyber security threats.

GROWTH AND INNOVATION

Cyberspace presents enormous opportunities for all Australian organisations. The Internet is an essential tool for businesses of all sizes. As a platform, it delivers existing services and products, as well as enabling the development of innovative technologies and new commercial opportunities. Equally, it underpins transformative change in the public, research and non-profit sectors.

In the Asia-Pacific region, disruptive business models and the technologies that enable them—such as big data analytics, mobile Internet, the Internet of Things and cloud computing—could create up to US$625 billion in economic activity per year by 2030, representing 12 per cent of the region's total projected GDP.

The Government's commitment to cyber security will **help businesses to diversify and develop** new markets, laying the foundations for a prosperous future. To take advantage of the growing global market for cyber security services, the Government will also **support Australia's cyber security sector to expand** and promote their capabilities to the global market. Domestically, strong cyber security services will encourage trust and confidence in Australian businesses operating online.

With better focused **cyber security research and development** that responds to the needs of industry and governments, Australia will generate investment and jobs and enhance our national cyber security. It will also make Australia a more attractive destination for business investment.

Australia will position itself as a location for **cyber security innovation** by establishing a Cyber Security Growth Centre, through the National Innovation and Science Agenda. Creating a national network of research and innovation, the Growth Centre will bring together Australian governments, businesses, start-ups and the research community to define and prioritise cyber security challenges that are both critical to national success and those for which Australia has a leading ability to build globally competitive solutions. The Growth Centre will also link to existing cyber security innovation hubs overseas. The Growth Centre and its network will help strengthen our cyber defences as well as growing business opportunities and creating jobs. This includes through its connection with other initiatives in this Strategy such as the joint cyber threat sharing centres.

Also through the National Innovation and Science Agenda, the Government is boosting the capacity of Data61—the Commonwealth Scientific and Industrial Research Organisation's (CSIRO) digital powerhouse—to propel cyber security innovation, with a particular focus on support for cyber security start-ups and technical capability

development internally and through Data61's partnerships with universities. This will include a cyber specific PhD scholarship program, with recipients spending time with Data61.

These initiatives complement other initiatives in the Government's National Innovation and Science Agenda which will also support cyber security businesses to grow and prosper. Similarly, all Australian innovations will benefit from improved protection from cyber-enabled intellectual property theft.
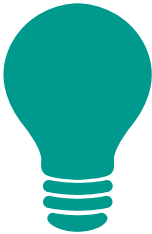
A CYBER SMART NATION

Underpinning the success of the other four themes in this Strategy is Australia's commitment to addressing the critical shortage of **skilled cyber security professionals**. Building on the Government's existing science, technology, engineering and mathematics (STEM) related initiatives, we will tackle this major problem through all levels of the education system, starting with the most urgent need in the tertiary sector.

The Government, together with the academic and research community and businesses, will co-design a model and then establish academic centres of cyber security excellence in universities to ensure graduates have the right skills and expertise. The centres of excellence will link with others around the world and also link with other initiatives in this Strategy such as the joint cyber threat sharing centres and the Cyber Security Growth Centre.

Australian governments, businesses and the research community will also work together to fix the cyber security skills pipeline to ensure more children at school study relevant subjects and to enable people at all stages of their careers to develop cyber security skills.

The Government will also further **improve national cyber security awareness** and work to ensure all Australians understand the risks and benefits of the Internet and how to protect themselves online, through sustained joint public-private awareness initiatives and education campaigns.

AUSTRALIA'S CYBER SECURITY STRATEGY AT A GLANCE

A NATIONAL CYBER PARTNERSHIP

Governments, businesses and the research community together advance Australia's cyber security.

Priority actions

Co-leadership: The Government and business leaders take the lead on co-designed, national cyber security initiatives, including through the Prime Minister holding annual cyber security meetings with business leaders.

Build stronger partnerships: The Government clearly identifies lead responsibilities and relocates the Australian Cyber Security Centre to engage with business more effectively.

Understand costs and effectiveness: The Government sponsors research to better understand the cost of malicious cyber activities to the economy.

STRONG CYBER DEFENCES

Australia's networks and systems are hard to compromise and resilient to cyber attacks.

GLOBAL RESPONSIBILITY AND INFLUENCE

Australia actively promotes an open, free and secure cyberspace.

GROWTH AND INNOVATION

Australian businesses grow and prosper through cyber security innovation.

Priority actions

Detect, deter and respond: Open jointly operated cyber threat sharing centres and an online cyber threat sharing portal. Tackle cyber threats with improved intelligence, analytic and response capability.

Raise the bar: Co-design voluntary cyber security governance 'health checks', national good practice guidelines, conduct joint exercisers and develop and leverage advanced technology to make Australia a harder target against cyber threats. Conduct cyber security assessments of Government agencies.

Priority actions

Champion an open, free and secure Internet: Advocate to retain an open, free and secure Internet, in the Indo-Pacific region and globally.

Shut down safe havens: Partner internationally to shut down safe havens and prevent cybercrime and other malicious cyber activity.

Build capacity: Help build capacity in our region and globally against malicious cyber activities.

Priority actions

Enable cyber security innovation: Drive investment in cyber security innovation through the Cyber Security Growth Centre and innovation network to strengthen cyber defences, grow our economy and create jobs.

Enable cyber security businesses to develop and expand: Support new businesses and promote the export of Australian cyber security products and services.

Enable cyber security research and development: Ensure our cyber security R&D is responsive to the challenges.

A CYBER SMART NATION

Australians have the cyber security skills and knowledge to thrive in the digital age.

Priority actions

Develop the right skills and expertise: Address cyber security skills shortages to develop a highly-skilled cyber security workforce, starting with academic centres of cyber security excellence and increasing diversity.

Raise national cyber security awareness: Lift all Australians' awareness of cyber risks and benefits through sustained joint public-private national awareness-raising initiatives.

"The Cyber Security Strategy underscores the powerful potential sparked by the cyber phenomenon. That potential revolves not just around Australia's national security, but equally around its economic wellbeing: it is unlocked by tackling these issues square on; by getting to grips with them in partnership across government, industry, academia and society; and in mastering their complexities and seizing their inherent possibilities."

Sir Iain Lobban, a member of the Cyber Security Review's Independent Panel of Experts

01

THE CYBER LANDSCAPE

CYBERSPACE IS A WORLD OF OPPORTUNITY...

The Internet based economy is growing twice as fast as the rest of the global economy. This is driven by a combination of surgi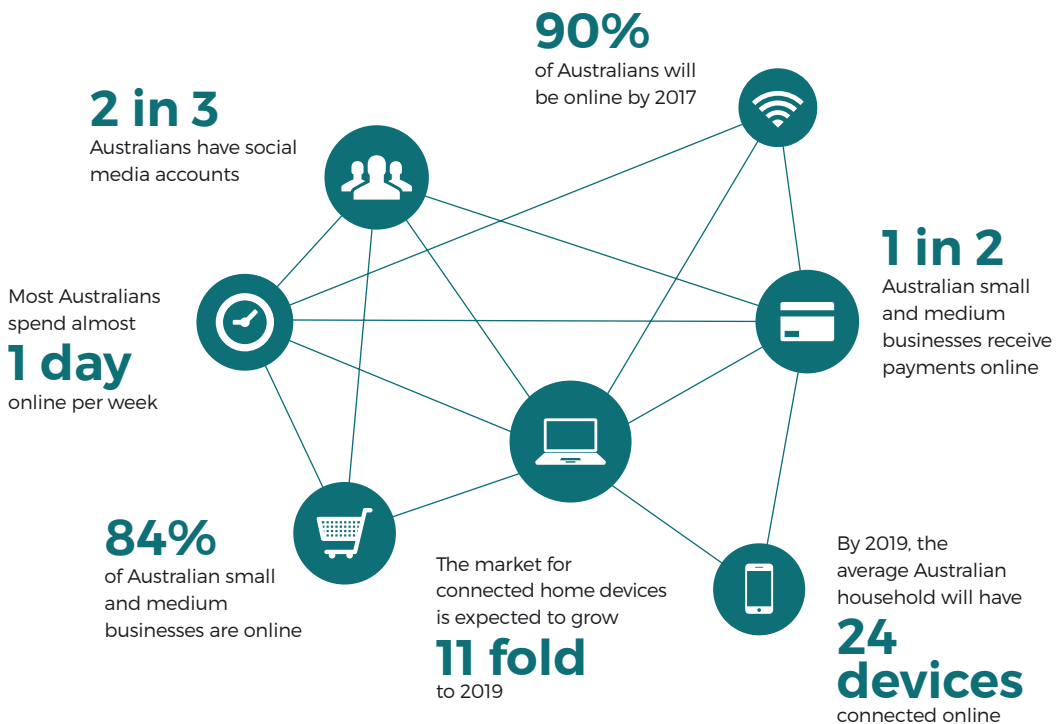ng business innovation and increased connectivity. Eight in ten Australians access the Internet daily. If poor cyber security erodes trust and confidence in cyberspace, the economic opportunity of a connected Australian economy will suffer. On the other hand, Australia stands to prosper significantly with reliable cyber security.

Australians have quickly embraced economic opportunities in cyberspace. In 2014 alone, the Internet based economy contributed $79 billion to the Australian economy (or 5.1 per cent of GDP).

This amount could grow to $139 billion annually (7.3 per cent of GDP) by 2020 as more devices, services and people are connected online.

Businesses and governments are also benefiting from improved online and mobile technology. They are using information gathered online to tailor products and services to individual needs. The rate of development of new commercial opportunities will accelerate as more and more of the things we own and use, such as fridges, cars, even pacemakers, are connected to the Internet and to each other. Once referred to as the 'Internet of Things', this phenomenon is now the 'Internet of Everything'.

Australians are becoming increasingly connected online

90%
of Australians will be online by 2017

2 in 3
Australians have social media accounts

1 in 2
Australian small and medium businesses receive payments online

Most Australians spend almost
1 day
online per week

84%
of Australian small and medium businesses are online

The market for connected home devices is expected to grow
11 fold
to 2019

By 2019, the average Australian household will have
24 devices
connected online

... BUT CYBER SECURITY THREATS ARE SERIOUS AND GROWING

As people and systems become increasingly interconnected, the quantity and value of information held online has increased. So have efforts to steal and exploit that information. Cyberspace, and the dynamic opportunities it offers, is under persistent threat.

Malicious cyber activity is a security challenge for all Australians. Australian organisations across the public and private sectors have been compromised by state-sponsored or non-state actors. Overseas, large multinational companies and government organisations have been targeted, losing substantial amounts of sensitive commercial and personal information or incurring major damage to their business and reputation.

Figures vary, but cybercrime is estimated to cost Australians over $1 billion each year.

Worldwide, losses from cyber security attacks are estimated to cost economies around one per cent of GDP per year. On this basis, the real impact of cybercrime to Australia could be around $17 billion annually. These costs are expected to rise. Government, telecommunications, resources, energy, defence, banking and finance sectors are likely to remain key targets for cyber criminals and malicious state actors alike.

The Australian Cyber Security Centre Threat Report 2015 says the cyber threat is undeniable, unrelenting and continues to grow. If an organisation is connected to the Internet, it is vulnerable to compromise—and the malicious cyber activities in the public eye are just the tip of the iceberg.

TYPES OF MALICIOUS CYBER ACTIVITY

Malicious cyber activities are wide ranging. They include activities designed to compromise the confidentiality, integrity or availability of computer networks or ICT systems or the information on them. The term 'cyber espionage' refers to theft of information for intelligence purposes. 'Cybercrime' refers to crimes directed at computers, such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software. It also includes crimes where computers are part of an offence, such as online fraud.

In this Strategy, the term 'cyber attack' refers to deliberate acts that seriously compromise national security, stability or prosperity by manipulating, denying access to, degrading or destroying computers or networks or the information resident on them. Other serious compromises are simply referred to as 'malicious cyber activity'.

Cyber adversaries are aggressive and persistent in their efforts to compromise Australian networks and information. They are constantly improving their tradecraft in an attempt to defeat our network defences and exploit new technologies.

They will also target the weakest link; if the network security of their primary target is robust, they will move to more easily compromised connected networks that could provide access to the primary target.

Further, the differences between some malicious cyber actors—such as organised criminal networks, state-sponsored actors and issue motivated groups—are becoming less distinct. For example, activity by some cyber criminals can be more sophisticated than those conducted by many nation states. This growing network of malicious actors is having a global impact.

Drivers of the rising cost of malicious cyber activity in Australia

Greater number of cyber security incidents

Almost one million Australians were estimated to be victims of identity theft online in 2014. Over 9,500 cyber crimes were reported to the Australian Cybercrime Online Reporting Network in its first three months of operation. The Australian Signals Directorate responded to 37 percent more government cyber security incidents in 2014 compared to previous years.

Greater number of targets

The range of possible targets is expanding from computers and phones to other devices connected to the Internet of Things, such as cars, fridges and medical equipment. There will be at least 50 billion connected devices by 2020.

Greater sophistication

Cyber attacks are becoming more sophisticated and previously unseen malicious activity, including infections to the firmware of hard drives, can now leave almost no trace. This saw software developers taking an average of 59 days to roll out patches for software vulnerabilities in 2014, compared to just four days in 2013.

INTRUSION VECTORS

An intrusion vector is the path or means an actor uses to gain access to a target. Common intrusion vectors include emails sent with malicious links and attachments; fake or manipulated websites that download viruses; removable media such as USB drives; unsecured wireless hotspots; and access through weak passwords.

Malicious actors can also use intrusion vectors to exploit human behaviour. Crafting an email containing malicious software based on a person's interests to entice them to open it is a vector, known as 'spearphishing'. These types of vectors are often referred to as social engineering: manipulating a person, overtly or otherwise, into performing actions or divulging confidential information. It can be in person or through cyberspace, such as grooming targets on social media.

WE CAN MAKE A DIFFERENCE

Australia has an opportunity to be a leader in the global cyber solution. As a stable and creative nation, Australia will help ensure the Internet is open, free and secure. In partnership with other countries, we can strengthen the foundations of international stability in cyberspace, enhance cooperative partnerships and build cyber security capacity.

Modelling in the US suggests the costs of managing cyber security risks for businesses are set to increase by 38 per cent over the next ten years, as further investment is required for cyber training and security tools. It is estimated that spending on cyber security of critical infrastructure in the Asia-Pacific region will reach US$22 billion by 2020, presenting a growing opportunity for Australia's cyber security industry.

This will deliver domestic dividends. Businesses are looking to invest in places with skilled workforces, engaged online consumers and simple regulatory environments that support innovation and security. Confidence in doing business online is critical. Getting cyber security right will mean Australia becomes a location of innovation and investment, a place where businesses start and grow, where organisations diversify and export and where all individuals can protect themselves online.

CYBER SECURITY ENABLES DISRUPTIVE TECHNOLOGY

In combination, many 'disruptive' technologies have significant potential to drive economic growth. In Southeast Asia alone, McKinsey has estimated that between mobile Internet, big data, the Internet of Things, automation of knowledge work and cloud technology, there is the potential to unleash some US$220 billion to US$625 billion in annual economic impact by 2030. But to fully realise these and other opportunities, these technologies and the infrastructure on which they operate must be trusted. Strong cyber security will enable this.

INTERNET OF EVERYTHING

It is estimated that by 2020 there will be at least 50 billion devices connected to the Internet globally. This explosion of connectivity will accelerate innovation in products and services, providing new business opportunities and new jobs.

However, the more connected 'things' are, the more targets there are for malicious actors. Part of the problem is that online security has not been considered in the design of many of the devices connected to the Internet. This has made it easier for malicious actors to disrupt and damage networks.

As an example of how vulnerable Internet connected devices can be, in 2015 the popular technology website Wired.com reported that security researchers had hacked into the electronics of a US car through its online entertainment system, changing its speed and braking capability before shutting the car engine down remotely. This demonstration led to the manufacturer having to provide software updates for 1.4 million US cars and trucks fitted with the same entertainment system.

Increased connectivity is also changing the relationship between consumers and businesses; it is fragmenting supply chains and business models. In turn, this will affect how people live and work, and how industries and economies perform.

CLOUD COMPUTING

Cloud Computing is a key feature of Australia's increasingly networked society. It provides individuals and businesses with greater data storage capacity, cost savings, convenience and flexibility. However, there are risks associated with cloud computing, including loss of control of data and problems recovering data.

The Government launched its Cloud Computing Policy in 2014, requiring Government agencies to adopt a 'cloud first' approach—where it is fit for purpose, provides adequate protection of data and delivers value for money. With the right measures, cloud computing can be used in both the public and private sector to improve cyber security, particularly for small organisations and businesses.

The Australian Cyber Security Centre has also provided guidance on secure cloud computing, including a list of Certified Cloud Services.

"Cyber security cannot be left to the Government alone to solve. Organisations and individuals play an essential role in effectively reducing cyber security risk."

Opinion article by Mike Burgess, Chief Information Security Officer, Telstra and member of the Cyber Security Review's Independent Panel of Experts

02

A NATIONAL CYBER PARTNERSHIP

GOVERNMENTS, BUSINESSES AND THE RESEARCH COMMUNITY TOGETHER ADVANCE AUSTRALIA'S CYBER SECURITY

To achieve our goal, the Government will:

- host annual cyber security leaders' meetings, where the Prime Minister and business leaders set the strategic cyber security agenda and drive this Strategy's implementation.

- streamline its cyber security governance and structures to improve interaction between the private and public sectors and will relocate the Australian Cyber Security Centre to allow for its growth and to enable the Government and the private sector to work more effectively together.

- work with the private sector and academic community to better understand the cost of malicious cyber activity to the Australian economy.

National co-leadership and cross-sectoral partnerships are essential for strong cyber security.

Cyber security needs to be driven from the top. Economic and national security imperatives mean that cyber security is a strategic issue for leaders—ministers, senior executives and boards—not just for IT and security staff. More strategic discussions between public and private sector leaders will focus on practical outcomes and elevate cyber security, both as a business risk and as a strategic opportunity rather than just as an operational matter.

Government and business leaders can do more to raise cyber security's prominence within their organisations, teams and peer groups. Including cyber security as a priority for corporate boards and international leaders will demonstrate that cyber security is a strategic priority for Australia.

ACTIONS SO FAR:

- The national Computer Emergency Response Team (CERT) Australia partners with over 500 businesses and advises on cyber security threats to the owners and operators of Australia's critical infrastructure. CERT Australia also works directly with other computer emergency response teams around the world. As part of their partnership arrangements, CERT Australia regularly convenes National and Regional Information Exchanges with businesses.

- The Cyber Security Challenge Australia is an annual cyber security competition for Australian tertiary students run by an alliance comprising Australian Government, business, academic and research professionals who are committed to supporting the next generation of Australian cyber security talent. The competition runs over 24 hours and tests the technical and communications skills of participants while promoting cyber security careers.

- Australian businesses and our research community are partnering to improve cyber security information sharing and innovation. Boards are increasingly considering cyber security issues. Some businesses share their data on malicious software with the Government while others are investing in research and development in cyber security technologies.

We are all responsible for our own activities in cyberspace, including being aware of the risks and how to protect ourselves and those who we are connected to.

More senior leaders of Australian organisations need to better understand cyber risk. Strengthened cyber security partnerships across the public and private sectors will give us a competitive advantage and increase Australia's potential as a modern, connected and innovative economy.

Under this Strategy, Government and business leaders will co-design national cyber security initiatives, including the Prime Minister holding annual cyber security meetings with business leaders. The meetings will bring together leaders from many sectors of the Australian economy to discuss how Government and business can collaborate to strengthen our economy and national security by building greater resilience to cyber security threats.

It is vital the public and private sectors work together to ensure individual and collective security, across the spectrum of cyber security challenges and opportunities that Australia faces.

CLEAR ROLES AND RESPONSIBILITIES

Organisations need easy and consistent interfaces with Government agencies on cyber security. A new streamlined Government cyber security structure will bring together disparate elements of both the policy and operational areas.

The Prime Minister will be supported by a Minister Assisting the Prime Minister for cyber security to lead the Government's work with business leaders to implement the initiatives.

In addition to the appointment of a Minister Assisting the Prime Minister on cyber security, the nation's cyber security governance will have three coordinated, strategic-level pillars.

First, the Department of the Prime Minister and Cabinet will strengthen its current lead role on cyber security policy and be the central point for policy issues to ensure a simplified Government policy interface for stakeholders. The Department will provide integrated oversight of the Government's cyber security policy and implementation of this Strategy. It will also prioritise the Government's activities against the Strategy's national cyber security objectives.

Government's Cyber Security Architecture
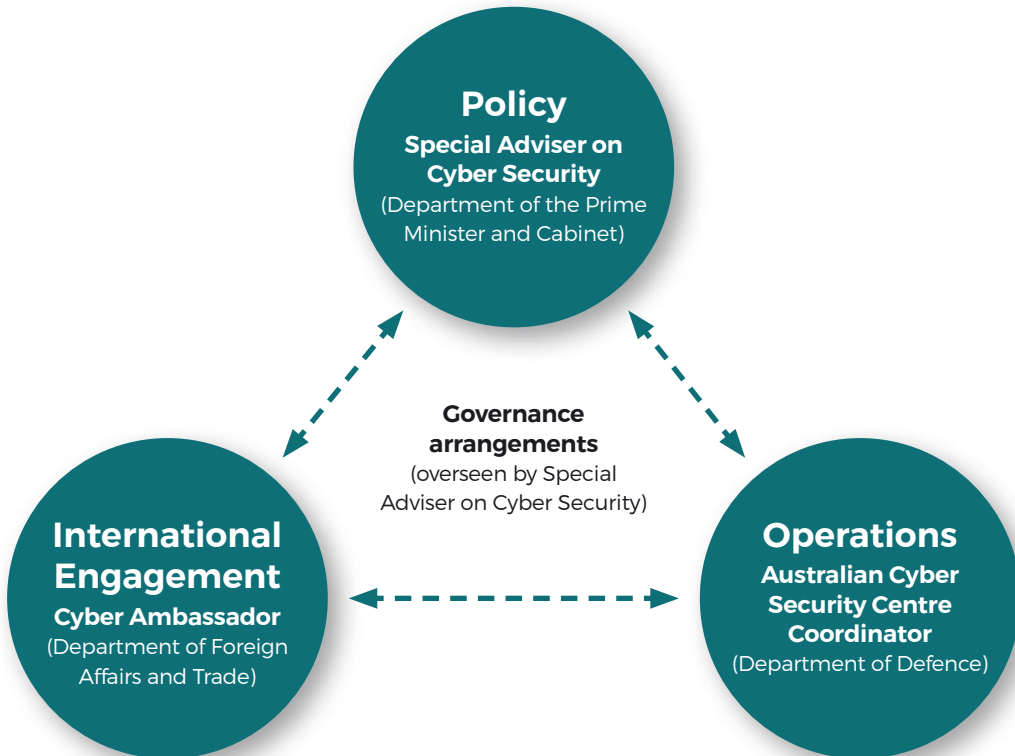
Leadership and advocacy of this work will be driven by a new position in the Department, the Prime Minister's Special Adviser on Cyber Security. The Special Adviser will lead the development of cyber security strategy and policy, provide clear objectives and priorities to operational agencies and oversee agencies' implementation of those priorities. The Special Adviser will also ensure the Government is partnering effectively with Australian governments, the private sector, non governmental organisations, the research community and international partners.

Second, the Australian Cyber Security Centre (ACSC), better guided by whole-of-nation

cyber security priorities, will continue to bring together the Government's operational cyber security capabilities and build on its world renowned cyber expertise to support a broader range of organisations at the operational level. In addition, ACSC outreach will be further improved and streamlined to make it easier for the private sector to interact. Recognising that Defence, in particular the Australian Signals Directorate, does much of the heavy lifting for the Government's role in defending Australia against malicious cyber activity, it will continue to lead the ACSC.

The ACSC will move to a new location. This will enable a more integrated partnership between the Government and its operational stakeholders, including businesses, the research and academic community and foreign partners collaborating with the ACSC.

Relocation may improve the ability of relevant ACSC agencies to quickly recruit new people and offer more flexible arrangements to continue to attract and retain a highly skilled workforce. It will enable the ACSC to accommodate new staff recruited as a result of the Strategy's implementation.

Third, the Minister for Foreign Affairs will appoint a Cyber Ambassador to lead Australia's international cyber effort. The Ambassador, working closely with and guided by the work of the Special Adviser on Cyber Security, will advocate for an open, free and secure Internet based on our values of free speech, privacy and the rule of law. This role will include ensuring Australia has a coordinated approach to cyber capacity building in our region, continuing to advocate against state censorship of the Internet and promoting our view that the opportunities provided by the Internet should be available to all people.

BETTER UNDERSTANDING COSTS AND BENEFITS

Statistical data on the national impact of cyber security compromises will enable Australian businesses and governments to make informed decisions when managing cyber risks. Data collection measures will help Australian governments and the private sector alike to make evidence based investment decisions that address the reality of cyber security threats to Australia's economy and security.

To help organisations better understand the impacts of malicious cyber activities, the Government will also sponsor research to better understand the cost of malicious cyber activity to the Australian economy.

"Fighting cyber threats needs shared action so decision-makers in governments, businesses and the community broadly have the information they need to protect themselves and our country."

Opinion article by Jennifer Westacott, Chief Executive of the Business Council of Australia and member of the Cyber Security Review's Independent Panel of Experts

03

STRONG CYBER DEFENCES

AUSTRALIA'S NETWORKS AND SYSTEMS ARE HARD TO COMPROMISE AND RESILIENT TO CYBER ATTACK

To achieve our goal, the Government will:

- establish a layered approach for sharing real time public–private cyber threat information through joint cyber threat sharing centres, initially piloted in a capital city, and an online cyber threat sharing portal.

- co-design national voluntary Cyber Security Guidelines with the private sector to specify good practice.

- update the Strategies to Mitigate Targeted Cyber Intrusions, published by the Australian Signals Directorate.

  continued...

- introduce national voluntary Cyber Security Governance 'health checks' to enable boards and senior management to better understand their cyber security status.

- support small businesses to have their cyber security tested.

- boost the capacity of the Australian Cyber Security Centre to respond to cyber security threats and cybercrime.

- update and align our cyber incident management arrangements with international partners and jointly exercise responses to malicious cyber activity with the private sector.

- support Government agencies to improve their cyber security, including guidance for Government agencies to manage supply chain security risks for ICT equipment and services.

Connected systems are complex and only as secure as the weakest link. This means that all Australians must work together to make sure our systems and information are among the hardest to compromise and that we have the best possible defences.

To better detect, deter and respond to malicious cyber activities, cyber threat information should be shared in real time between and within Australia's public and private sectors. Both have unique information to contribute to the threat picture. It is only by combining our knowledge that we can comprehensively understand cyber security threats to Australia and how to counter them.

It is equally important to deter malicious cyber activities by better understanding the threat and bringing the perpetrators to justice. Due to the global nature of malicious online activities, tackling cybercrime will involve both increasing the numbers and improving the criminal intelligence capacity and skillsets of law enforcement officers at home, as well as partnering with law enforcement and other agencies abroad.

Australia's defensive and offensive cyber capabilities enable us to deter and respond to the threat of cyber attack. Any measure used by Australia in deterring and responding to malicious cyber activities would be consistent with our support for the international rules-based order and our obligations under international law.

ACTIONS SO FAR:

- The Australian Cyber Security Centre, opened in 2014, brings together cyber security capabilities across the Australian Government to collaborate and share threat information.

- Under the National Plan to Combat Cybercrime, Australian governments committed to taking concrete steps to tackle cybercrime in six priority areas, including community education.

- The Australian Cybercrime Online Reporting Network (ACORN) provides advice on how to recognise and avoid cybercrime. ACORN allows individuals to report cybercrimes that breach Australian law.

- The Australian Signals Directorate maintains world-leading cyber security advice in its Strategies to Mitigate Targeted Cyber Intrusions. The strategies are based on the Directorate's analysis of reported security incidents and identified vulnerabilities.

- The Australian Media and Communications Authority facilitates the Australian Internet Security Initiative, a voluntary public-private partnership helping to reduce malicious software and service vulnerabilities occurring on Australian Internet protocol (IP) address ranges.

- Recognising the particular importance of secure telecommunications networks, the Government is working with telecommunications companies to manage supply chain risks by providing advice on protecting their networks and the information stored and carried across them. This includes work the Government is doing on Telecommunications Sector Security Reform to establish more formal and comprehensive arrangements to better manage national security risks of espionage, sabotage and interference.

DETECT, DETER AND RESPOND

Cyber adversaries are aggressive and persistent in their efforts to compromise Australian networks and information. They are constantly improving their methods in an attempt to defeat our network defences and exploit new technologies. Cyber adversaries will target the weakest link if the network security of their primary target is robust.

Strong cyber security ensures organisations can better detect malicious cyber activity. It can also be an effective deterrent by increasing the effort necessary for an attacker to succeed. Further, it can ensure that when malicious activity does occur, the consequences are reduced and the extent of the activity contained effectively.

Businesses own and operate most of the infrastructure in cyberspace. They have information about malicious cyber activities on their networks and systems that is not readily available to Government agencies. On the other hand, the Government has access to intelligence and other restricted information about cyber security threats that is not readily available to businesses. Equally, businesses want to share information with each other using the Government as the honest broker.

Organisations, public and private, must work together to build a collective understanding of cyber threats and risks through a layered approach to cyber threat sharing. By securely sharing sensitive information and working together—in real time where possible—we can build a stronger collective understanding and ability to analyse and predict cyber security threats. This includes detection of patterns of malicious cyber activity and implementing adaptive and behavioural analysis to enable an epidemiological approach to responding to cyber threats. Pooling our resources is also more efficient and will help develop quicker responses to compromises and build national resilience. We can draw from the positive lessons learned from other successful cyber security partnerships, such as AusCERT.

AUSCERT

AusCERT has helped its members prevent, detect and respond to cyber attacks since 1993. As a membership based, independent, self-funded, not-for-profit security team based at The University of Queensland, AusCERT has a national focus across industry and government and a national and global reach. AusCERT maintains a large network of trusted contacts with computer emergency response teams in Australia and overseas, including CERT Australia, Australia's national CERT. AusCERT contributes to initiatives to help improve cyber security through its services to members, assistance to international CERTs, partnerships, submissions to government and participation in Australian and international cyber security forums.

The Australian Cyber Security Centre already shares threat information with the private sector and is improving its links to critical infrastructure providers. To share sensitive information quickly with a broader range of businesses, the Government will establish joint cyber threat sharing centres, co-designed with the private sector, in key capital cities to co-locate businesses and the research community together with state, territory and commonwealth agencies.

The joint cyber threat sharing centres will produce advice that organisations can use to take practical steps to improve their cyber security. The first step will be piloting the operating model for centres. Business and government partners will co-design principles on how information is shared. Based on the outcomes of the pilot, further centres will be opened in key capital cities.

THE AUSTRALIAN CYBER SECURITY CENTRE (ACSC)

The ACSC, opened in 2014, is a world-leading collaborative initiative. The ACSC brings together the Australian Government's operational cyber security capabilities in one location to share threat information and combat sophisticated cyber security threats. The ACSC's partner agencies include:

- Australian Crime Commission
- Australian Federal Police
- Australian Security Intelligence Organisation
- Australian Signals Directorate
- Computer Emergency Response Team (CERT) Australia
- Defence Intelligence Organisation

In July 2015, the ACSC released its first public Cyber Security Threat Report outlining the range of cyber adversaries targeting Australian networks, their motivations, the nature of the attacks and their impact. This was an important first step in sharing more information on cyber security threats. These reports will be updated and published at least annually as part of the approach to cyber threat sharing. The ACSC also provides advice on how organisations can defend themselves online and undertakes customer surveys to assess the maturity of cyber security practices.

To meet the needs of an even broader set of businesses and organisations, including small to medium businesses, the Government will also co-design with the private sector an online cyber threat sharing portal. It will enable participants in joint cyber threat sharing centres to quickly publish threat information and practical advice that Australian organisations can use to strengthen their cyber defences. Members of the portal will be able to collaborate online and share threat information and response options.

As part of the co-design of the cyber threat sharing model, linkages to global cyber security threat sharing initiatives and incentives for businesses to share information and improve cyber security will also be explored. This includes examining legislative impediments to sharing.

A layered approach to cyber threat sharing

Australian Cyber Security Centre
The Australian Government partners with key businesses within the Australian Cyber Security Centre to share highly classified information on critical services

Joint Cyber Threat Centres
Australian governments, businesses and the research community partner in joint cyber threat sharing centres in key capital cities to exchange sensitive cyber threat information

Online cyber threat sharing portal
A broad range of organisations share information on a secure, online cyber threat sharing portal, including the results of analysis by the joint cyber threat sharing centres

The Government is committed to equipping the Australian Cyber Security Centre with the resources and tools it needs to fight the rising tide of malicious cyber activity and keep our cyberspace safe. The Government will boost the capacity of the ACSC agencies to tackle cyber security threats by:

• increasing the capacity of the national Computer Emergency Response Team (CERT) Australia to scale up their work with Australian businesses, in particular those providing critical services. The additional capacity will also improve CERT Australia's technical capability to support businesses and to partner internationally to prevent and shut down malicious cyber activity; and

• funding new specialist officers for the Australian Crime Commission and the Australian Federal Police to tackle cybercrime. There will also be new training, including new modules in entry colleges and eLearning for existing personnel, which will boost the digital investigation skills of specialist officers to create a cyber smart law enforcement and criminal intelligence workforce.

The Government will also explore with states and territories how best to ensure that law enforcement officers receive the training they need to fight cybercrime across the nation.

The technical environment is becoming more complex. Technologies that underpin and are used within cyberspace rapidly evolve and more traditional technologies are being used for new purposes. For example, as encryption technology becomes cheaper and more widely available, there is an opportunity for all users to access this technology to secure information and improve their cyber security. However, there is also a growing trend for groups and individuals to use encryption to hide illegal activity and motivate others to join their cause.

The Government supports the use of encryption to protect sensitive personal, commercial and government information. However, encryption presents challenges for Australian law enforcement and security agencies in continuing to access data essential for investigations to keep all Australians safe and secure. Government agencies are working to address these challenges.

While new cyber security vulnerabilities are emerging every day, many are becoming increasingly difficult to identify. The Government will increase the capacity of the Australian Signals Directorate to identify new and emerging threats to Australia's cyber security and improve intrusion analysis capabilities. Through the 2016 Defence White Paper, the Government is also boosting Defence's cyber security capacity and capability—this includes new resources to strengthen Defence's cyber capabilities to protect itself and other critical Australian government systems from malicious cyber intrusion and disruption.

WHAT IF MY SYSTEM HAS BEEN COMPROMISED?

Businesses are encouraged to contact the Computer Emergency Response Team (CERT) Australia through the Australian Cyber Security Centre if they think they have been the target of a malicious cyber intrusion, particularly if there has been a threat to infrastructure. Faster identification may help to minimise the extent of potential damage. In time, the layered approach to threat sharing will help streamline reporting of incidents and build a more detailed picture of cyber threats to Australia.

The Government must also be ready to respond to incidents when they occur. Cyber incidents do not necessarily need a cyber response and the Government can draw on a range of options, including law enforcement, diplomatic, economic or even—as a last resort—military responses to a cyber attack. In order to ensure we are prepared to respond to a significant cyber security event and to improve our existing exercise practices, the Government will work with other governments, businesses and international partners to expand our existing cyber incident management arrangements and exercise program to ensure we can operate together in a crisis.

CYBERSTORM EXERCISE

CyberStorm is an international cyber security exercise program led by the United States. Each successive CyberStorm has grown in size and complexity, with over 1000 players participating globally in CyberStorm V in 2016. Participating in CyberStorm allows Australia to assess its own capabilities using real world scenarios. It also strengthens our relations with international peers and tests these operational relationships in real time. Cyber security exercises are one of the most effective tools businesses can employ to demonstrate potential whole-of-business impacts of a cyber attack,

RAISE THE BAR

While detecting and responding to cyber intrusions is important, even more important is to harden our networks and systems and make them less vulnerable to intrusions. In this case, prevention is definitely better than the cure.

Although some organisations may be implementing international cyber security standards that all organisations can achieve, others are not doing so. In our interconnected world, a solid baseline of cyber security practice is critical to achieving confidence online.

Self-regulation and a national set of simple, voluntary guidelines co-designed with the private sector will help organisations improve their cyber security resilience. As suggested by the private sector, these guidelines will be based on the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions. These strategies will continue to be updated to keep pace with evolving technologies and innovative responses to cyber security challenges.

While in its infancy in Australia, the rapidly growing cyber insurance market may help enforce improved cyber security performance.

ASX 100 listed businesses will have the opportunity to improve their cyber security governance by participating in voluntary governance 'health checks'. The governance health checks will enable boards and senior management to better understand their cyber security status and how they compare to similar organisations. In time, these health checks (similar to the United Kingdom's FTSE 350 governance health checks) will be available for public and private organisations, tailored to size and sector.

Small businesses often find it challenging to allocate resources to do cyber security well. Without adequate cyber security they can become the soft underbelly or back door into connected organisations. The Government will provide support for small businesses to have their cyber security tested by certified practitioners.

The Government will also support the Council of Registered Ethical Security Testers (CREST) Australia New Zealand to expand its certification of information security testing services.

CREST AUSTRALIA NEW ZEALAND

The Council of Registered Ethical Security Testers (CREST) Australia New Zealand is a not-for-profit cyber security standards organisation where member companies become CREST Approved if they meet appropriate governance standards. CREST Australia New Zealand then provides accreditation and certification for employees and contractors of CREST Approved Member Companies through practical exams in penetration testing and soon other in-demand areas of cyber security. CREST certified practitioners, while being attached to CREST Approved Companies with good governance, give businesses in Australia and the region the confidence that testing of the cyber security of their networks and systems is done by skilled cyber security professionals.

Cyber espionage activities target Australian Government networks almost daily and as a result Government systems have been compromised. In 2013, the Australian National Audit Office completed an audit of seven agencies' compliance with the Government's cyber security policies and found most fell well short. These Government agencies are responding to the audit in order to continue to improve security.

To take action to better protect itself, the Government will:

- undertake a rolling program of independent assessments of Government agencies' implementation of the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions;

- fund independent cyber security assessments of Government agencies at higher risk of malicious cyber activity and develop a framework that helps those agencies address findings; and

- increase the capacity of the Australian Signals Directorate to conduct vulnerability assessments of Government agencies and provide technical security advice on emerging technologies and vulnerabilities.

These assessments will help ensure appropriate action is being taken to manage cyber risks and that agencies have the right measures in place to respond to malicious cyber activity. The results from these assessments will inform further action to ensure all Government agencies are a harder target for cyber attack. The work on emerging technologies will also help inform the Australian Cyber Security Centre's advice to the public and private sectors.

ICT supply chains have evolved with a diversity of ICT products and services being provided by a broad range of vendors. Products are routinely deployed and serviced globally. This has increased competition and lowered costs. As a nation with limited local ICT manufacturing, Australia has little control over the manufacture of these products and relies on services from a range of domestic and international organisations. A diverse and global supply chain can introduce risk.

The Government will develop guidance for its agencies to consistently manage supply chain security risks for ICT equipment and services. In time, this work will be used to help inform the private sector.

"The openness of the Internet lies at the heart of its role as an economic driver, as well as the basis for its contribution to social life. It connects people and ideas; it eliminates distance and time. It is a libertarian force for good."

Minister for Foreign Affairs, The Hon Julie Bishop MP, at the
2013 Global Conference on CyberSpace in Seoul

04

GLOBAL RESPONSIBILITY AND INFLUENCE

AUSTRALIA ACTIVELY PROMOTES AN OPEN, FREE AND SECURE CYBERSPACE

To achieve our goal, the Government will:

· appoint Australia's first Cyber Ambassador.

· publish an international cyber engagement strategy.

· champion an open, free and secure Internet that enables all countries to generate growth and opportunity online.

· partner internationally to shut down safe havens and prevent malicious cyber activity, with a particular focus on the Indo-Pacific region.

· build cyber capacity in the Indo-Pacific region and elsewhere, including through public–private partnerships.

Cyber security is a critical issue for Australia's international cooperation. Cyberspace is already a core foreign policy issue and a central theme of Australia's diplomatic efforts. Developing norms of state behaviour, the application of international law, Internet governance and cyber innovation are regularly discussed at multilateral forums and by Presidents and Prime Ministers.

Australia needs to partner internationally to ensure our cyber engagement advances our security and economic interests, as well as our values. The Government will publish an international engagement strategy to help guide our bilateral and regional cooperation on cyber security.

But the private sector and research community can and must be part of the international cyber agenda—only then can we promote all Australians' interests in cyberspace.

Australia advocates for an open, free and secure Internet based on our values of free speech, privacy and the rule of law. We will continue to promote that opportunities provided by the Internet be available to all people, advocating against state censorship of the Internet. The newly appointed Cyber Ambassador will lead Australia's efforts on this front together with a coordinated approach to cyber capacity building in our region.

ACTIONS SO FAR

- Australia chaired the United Nations Group of Governmental Experts in 2012–13 that found existing obligations under international law are applicable when operating in cyberspace.

- Australia has played an important role in advancing risk reduction and conflict prevention through leading on the ASEAN Regional Forum cyber work plan adopted by Ministers in August 2015.

- In 2015, Australia joined the Freedom Online Coalition—a partnership of 29 governments working to advance Internet freedom.

- The Australian Federal Police works with policing agencies throughout the Indo-Pacific region on training and capacity building initiatives to counter cybercrime. For example, the Cyber Safety Pasifika initiative is a collaborative project between the Pacific Islands Chiefs of Police and the Australian Federal Police. It has now been launched in 14 Pacific Island countries and has trained 40 Pacific Island instructors to deliver cyber safety education in their own countries and mentoring support in other Pacific Island countries. Over 72,000 children and young people in the Pacific have now attended its education and awareness workshops.

- In 2013, Australia joined the Council of Europe Convention on Cybercrime, otherwise known as the Budapest Convention. The Convention codifies what constitutes a criminal offence in cyberspace and streamlines international cybercrime cooperation between signatory states.

- The national Computer Emergency Response Team (CERT) Australia presently chairs the steering committee of the Asia Pacific Computer Emergency Response Team (comprising 28 teams from 20 economies across the region) and shares threat information with other response teams around the world.

- The Australian Attorney-General's Department provides assistance to Pacific Island countries to reform their criminal justice frameworks to address cybercrime.

- In parallel to our cyber security partnerships, the Government is enhancing cooperation with international partners to detect and prevent terrorists' use of the Internet and counter violent extremism online. This includes Australia being a lead partner in the East Asia Summit and Asia-Pacific Economic Cooperation's efforts to counter online extremism and combat online terrorist propaganda.

AN OPEN, FREE AND SECURE INTERNET

Several countries currently remain determined to impose constraints on the open nature of the Internet.

Australia has consistently advocated for an open, free and secure Internet based on our values of freedom of speech, right to privacy and rule of law. Australia will continue to promote the opportunities provided by the Internet to be available to all, advocating against state censorship of the Internet.

Three core principles guide Australia's international cyber engagement:

- The current way the Internet is governed, involving the private sector and the community as equal partners with governments, is the most effective model. This multi-stakeholder model of Internet governance delivers economic benefit and social opportunity while balancing fundamental human rights, such as freedom of expression and privacy.

- State behaviour in cyberspace is governed by international law and reinforced by agreed norms of state behaviour and practical confidence building measures to reduce the risk of conflict.

- Developing cyber capacity internationally helps to close the digital and economic divide between developed and developing nations and, in doing so, enhances Australia's national security and export opportunities.

By increasing mutual understanding, we can also help to reduce tension between states and the risk of miscalculation. Australia will continue to promote peacetime norms for acceptable state behaviour in cyberspace, which include that states should:

- prevent and refrain from online activity that damages or impairs critical infrastructure;

- facilitate (and not hinder) the critical work of other national Computer Emergency Response Teams in protecting online security;

- live up to their responsibilities in investigating and policing malicious activity online emanating from their national territory and responding to requests for cooperative action; and

- not conduct or knowingly support cyber-enabled theft of intellectual property, with the intent of providing competitive advantage to companies or commercial sectors.

CYBER POLICY DIALOGUES

In 2014-15 Australia opened formal multi-agency cyber policy dialogues with China, India, Japan and the Republic of Korea to strengthen our partnerships in Asia. Australia also has a longstanding cyber policy dialogue with New Zealand since 2012.

These dialogues provide a foundation for practical cooperation, allowing us to strengthen existing bilateral ties, share valuable cyber threat information, exchange views and advocate for Australia's interests. For example, the Government uses the dialogues to promote an open, free and secure Internet and emphasise the importance of norms of behaviour for stability in cyberspace.

SHUT DOWN SAFE HAVENS

Partnerships between Australia and other countries are critical to developing mutual confidence and ensuring there are no safe havens for cyber criminals and other malicious cyber actors. They also allow us to work internationally to stop cyber attacks and track down perpetrators. Australia will continue to invest in these relationships and in raising the cyber security capacity of our region.

Most cybercrime originates from overseas. Partnering internationally to prevent and shut down malicious cyber activity and build

capacity helps target cyber security risks at their source and spreads resilience, paying dividends for Australia's cyber security.

It also helps protect Australian businesses.

Australia will work even more closely with and, where necessary, support our international partners in preventing cyber attacks and shutting down safe havens for cybercrime.

BUILD CYBER CAPACITY NEAR AND FAR

Practical action and partnership are critical to tackling cyber criminals and to prevent them from proliferating, particularly in our region. A comprehensive, joined-up approach on cyber security by Australia and our partners must also be grounded in mutual trust.

The Government will increase the extent of our activity and partner internationally, particularly in the Indo-Pacific region, to help build capacity against malicious cyber activities.

This will include sharing techniques to combat cybercrime, and enabling close collaboration between national computer emergency response teams.

SHARING AUSTRALIA'S EXPERTISE IN CYBER SECURITY

In 2015 at the Global Conference on CyberSpace in The Hague, Australia became a founding partner of the Global Forum on Cyber Expertise to improve cyber capacity building (e.g. sharing our skills with and learning from other countries). Through the Forum, Australia will bring its expertise and strengths to partner with countries in our region to mitigate cyber attacks.

"A strong cyber security capability is crucial for Australia to be a global leader as the world economy enters the next wave of digital enablement."

John N. Stewart, Senior Vice President and Chief Security and Trust Officer, Cisco and member of the Cyber Security Review's Independent Panel of Experts

O5

GROWTH AND INNOVATION

AUSTRALIAN BUSINESSES GROW AND PROSPER THROUGH CYBER SECURITY INNOVATION

To achieve our goal, the Government will:

- establish a Cyber Security Growth Centre with the private sector to coordinate a national cyber security innovation network that pioneers cutting edge cyber security research and innovation.

- promote Australian cyber security products and services for development and export, with a particular focus on the Indo-Pacific region.

- work with business and the research community to better target cyber security research and development to Australia's cyber security challenges.

Future economic growth in Australia will be boosted by access to new markets and the development of new forms of wealth creation. Disruptive technologies will open up new business opportunities, but many of these depend on trust and confidence in the security of cyberspace. Getting cyber security right will mean Australia is a secure and dynamic location for business diversification and investment.

Cyber security is one of the fastest growing sectors in many national economies and Australia is well placed to use our home-grown capabilities to develop business opportunities in this increasingly connected world.

Our domestic cyber security sector, though small, has a good reputation internationally. To ensure we capitalise on these assets, the Government will help create the right environment to incubate cyber security research, development and start-ups.

RECENT ACHIEVEMENTS

Australia's domestic innovation and research industry is well regarded, supported by targeted efforts from both government and the private sector.

· Cyber security is one of nine Government National Science and Research Priorities.

· Australian businesses are taking advantage of cyber opportunities. In recent years, home-grown cyber security online businesses have won Australian Export and Innovation awards for their export success and their unique products and services.

· Cyber security innovators are winning international acclaim—and out-competing overseas counterparts for venture capital to commercialise solutions to complex cyber security challenges.

ENABLE CYBER SECURITY BUSINESSES TO DEVELOP AND PROSPER

Cyberspace presents enormous opportunities for Australian businesses. We bring technical innovation, a skilled workforce and the experience gained from early adoption of technology across our economy. We need to harness this expertise and achieve scaled success for Australia's economy and security to benefit from our strong cyber security R&D foundations.

More broadly, focused cyber security services will support trust and confidence in

Australian businesses operating online. The Government's commitment to cyber security will help businesses diversify and foster new markets, laying the foundations for a prosperous future. The Government will also promote Australia's cyber security sector to the expanding global market for trusted cyber security services, which at around eight per cent a year, is expanding twice as fast as global economic growth.

SUPPORT FOR ENTREPRENEURS

The National Innovation and Science Agenda is helping innovators commercialise good ideas. A number of the initiatives support start-ups and entrepreneurs, including:

• enhancing the visa system to attract the best and brightest entrepreneurial talent and skills to Australia

• making changes to the tax treatment of Early Stage Venture Capital Limited Partnerships to attract more investment into our high potential start-ups

• promoting investment in innovative, high-growth potential start-ups by providing concessional tax treatment for investors

• the Incubator Support Program, growing the next generation of innovative and high performing Australian businesses

• investing $36 million over five years in a Global Innovation Strategy to improve Australia's international innovation and science collaboration

• supporting commercialisation of research from CSIRO, other research organisations and universities through an early stage innovation fund.

ENABLE CYBER SECURITY R&D AND INNOVATION

The Government is investing over $30 million to establish an industry-led Cyber Security Growth Centre to create business opportunities for Australia's cyber security sector and improve Australian businesses' cyber security.

The Cyber Security Growth Centre was announced in December 2015 as part of the Government's National Innovation and Science Agenda and will develop a national plan to grow Australia's cyber security sector. It is part of the Government's Industry Growth Centres initiative and will coordinate cyber security research and innovation for national benefit and enable Australia to become a global leader in cyber security solutions and services. This will generate investment and jobs for the economy.

In addition, the Cyber Security Growth Centre will provide strategic coordination of a national cyber security innovation network that links cyber security innovation hubs and cyber security R&D around Australia and early-adopter businesses and government agencies. It will provide the national mechanism for cross-sector collaboration and investment in nationally-significant cyber security infrastructure and frameworks that are not singularly commercially-viable. To take advantage of the 'fourth industrial revolution' generated by cyberspace, governments, businesses and the research community will come together to link Australian research and start-up incubation with commercial opportunities. The Growth Centre will also work to improve the workforce skills of the sector and seek opportunities for the Australian cyber security sector to access global markets. This will help grow Australia's cyber security sector and help all Australians and businesses be more secure online.

Data61, CSIRO's digital powerhouse, will also contribute to the national cyber security innovation network through its cyber security research and collaboration with the private sector and by connecting the network internationally through initiatives such as the Security Innovation Network (SINET).

The industry-led Growth Centre and its innovation network will support and inform the Government's National Science and Research Priority on cyber security by guiding and leveraging existing government measures at the federal, state and local levels to improve research commercialisation, business innovation and competitiveness.

For example, the Growth Centre will identify cyber research and technology gaps or priorities for industry, and inform the science and research community of industry needs and commercial opportunities. It will also work with other Growth Centres to identify cyber security challenges in other sectors.

The Growth Centre will also complement other initiatives under this Strategy, including the joint cyber threat sharing centres, to support solutions to emerging cyber security threats; and academic centres of cyber security excellence (discussed in the next chapter), by providing tertiary students with hands on experience in solving cyber security challenges before they graduate.

CYBER SECURITY
GROWTH CENTRE

IMPROVED ENGAGEMENT
BETWEEN RESEARCH AND BUSINESS

IMPROVED MANAGEMENT AND **WORKFORCE SKILLS**

IMPROVED ACCESS TO INTERNATIONAL MARKETS
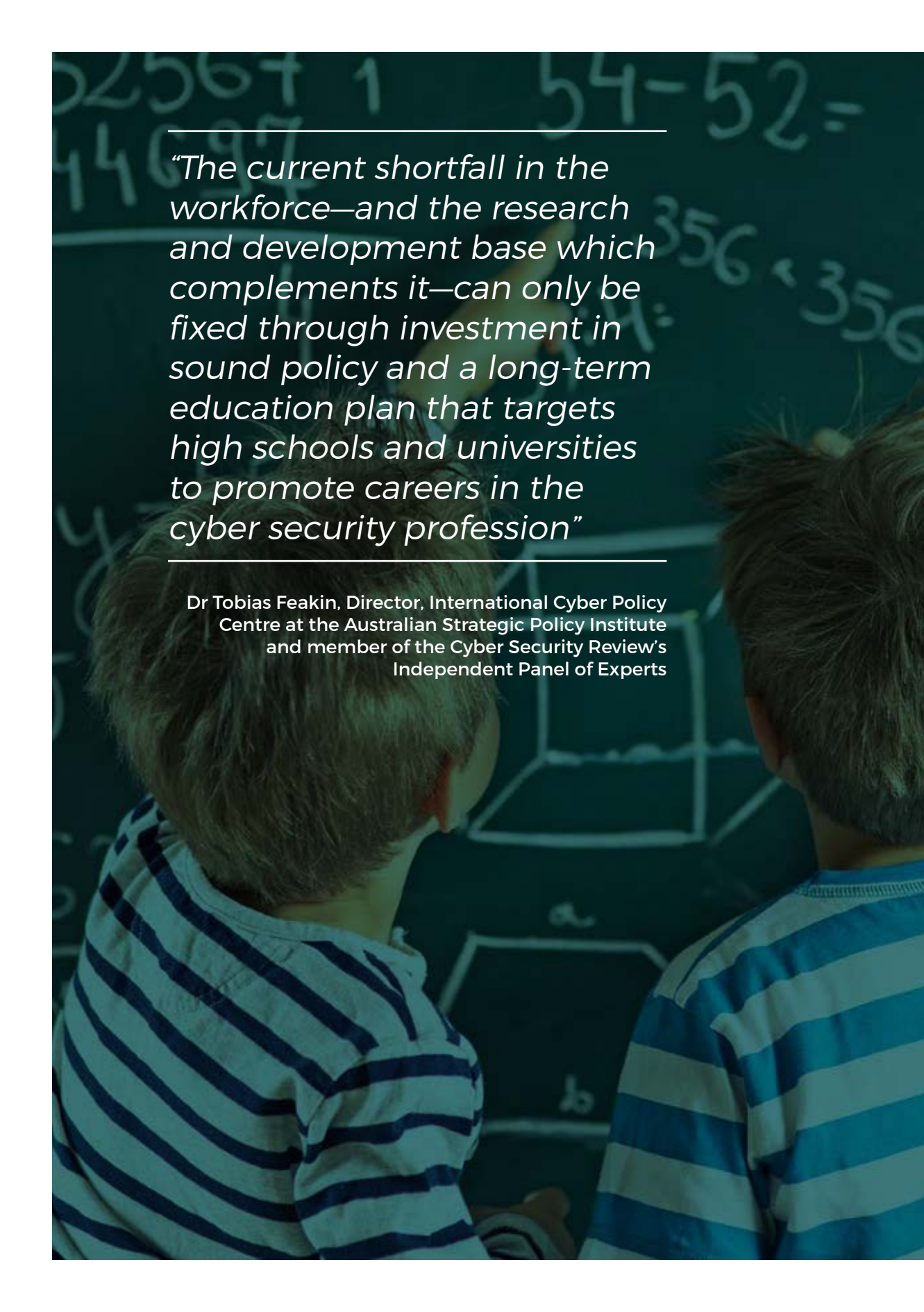
REGULATORY REFORM

DATA61—AUSTRALIA'S LARGEST DATA INNOVATION GROUP

Formed in 2015, Data61 has already established an impressive network of partnerships across industry, government and academia, quickly becoming Australia's largest data innovation group.

To capitalise on the emerging data-driven economy, Data61 is developing 'leap ahead' technologies to enable industry and government to be at the cutting edge of cyber security. The strategic objectives for Data61 are closely aligned with this Strategy, reiterating the importance of cyber security in a data-driven future.

Data61's mission is to help Australia create new technology-based industries. Cyber security is one of those industries and underpins all others. To achieve this, Data61 is focused on national alignment with global context, fostering a global innovation network—connecting academia, corporations, start-ups, governments, investors and entrepreneurs around the world. In 2016, Data61 will also bring the Security Innovation Network, SINET, to Australia, a 'super-connector' for cyber security innovation based in the US. The Australian network, to be known as SINET61, will connect to a series of global activities and will build on SINET's existing annual events in Silicon Valley, New York, Washington DC and London that bring together cyber security entrepreneurs and start-ups with venture capitalists and angel investors.

"The current shortfall in the workforce—and the research and development base which complements it—can only be fixed through investment in sound policy and a long-term education plan that targets high schools and universities to promote careers in the cyber security profession"

Dr Tobias Feakin, Director, International Cyber Policy Centre at the Australian Strategic Policy Institute and member of the Cyber Security Review's Independent Panel of Experts

A CYBER SMART NATION

AUSTRALIANS HAVE THE CYBER SECURITY SKILLS AND KNOWLEDGE TO THRIVE IN THE DIGITAL AGE

To achieve our goal, the Government will:

- address the shortage of cyber security professionals in the workforce through targeted actions at all levels of Australia's education system, starting with academic centres of cyber security excellence in universities and by increasing diversity in this workforce.

- work with the private sector and international partners to raise awareness of the importance of cyber security across our community.

Like many other nations, Australia is suffering from a cyber security skills shortage. These particular skills are essential in our connected, technology-enabled world and they are fundamental to the success of this Strategy. But these same skills are in increasingly short supply—for example, the information security field is expected to see a worldwide deficit of 1.5 million professionals by 2020.

Many Australians and organisations are also simply unaware of the risks they face in cyberspace. Most of us lock our front doors and take care of our belongings, but we do not take the same degree of care with our devices and online information. The Government is committed to equipping Australians with the right cyber security skills and raising levels of cyber security awareness so we can all benefit from the opportunities in cyberspace.

ACTIONS SO FAR

- Stay Smart Online provides useful advice to help everyone protect personal and financial information online. The Government is coordinating cyber security awareness internationally and has aligned Stay Smart Online Week with the global Cybersecurity Awareness Month coordinated by the US.

- The Australian Competition and Consumer Commission operates SCAMwatch, providing information to individuals and businesses on identifying and reporting scams.

- The Office of the Children's eSafety Commissioner was established to provide information and resources to help guide children and young people towards safe, enjoyable experiences online, coupled with a comprehensive complaints system to assist children who experience serious cyber bullying.

- The private sector has also invested in developing cyber skills. Box Hill Institute of TAFE in Victoria is developing a twelve-month cyber security apprenticeship with a Certificate IV qualification in conjunction with the private sector. Australian banks and telecommunications businesses have partnered with universities to fund scholarships for students to study technology courses, including cyber security degrees.

- The Australian Cyber Security Research Institute (ACSRI) is Australia's first coordinated strategic research and education effort between Government agencies, the private sector and researchers. It seeks to support the Government's focus on cyber security by bringing together a collaborative network to deliver an Australia-wide approach to respond to cyber threats and improve opportunities for developing highly skilled cyber security professionals.

Demand in Australia for cyber security services and related jobs—such as legal services, insurance and risk management—will grow by at least 21 per cent over the next five years. There will be significant employment and career opportunities for those with appropriate skills.

However, the public and private sectors cannot fill their cyber security vacancies.

The situation appears to be worsening—the take-up of ICT-related university degrees (often a precursor for cyber security professionals) has halved over the last decade and graduation rates have dropped. There are several potential explanations for this, including the type and number of courses currently available, and insufficient student awareness of job opportunities.

DEVELOP THE RIGHT SKILLS AND EXPERTISE

To build tomorrow's workforce, the Government will work in partnership with the private sector and academic institutions to improve cyber security education at all levels of the education system. This will help to ensure Australia develops a workforce with the right skills and expertise that can help all Australians take full advantage of the opportunities in cyberspace.

The most urgent need is for highly-skilled cyber security professionals. Academic centres of excellence will enhance the quality of cyber security courses, teachers and professionals in Australia. The standard for gaining accreditation as a centre will be high and maintained through continual rigorous assessment.

The centres will deliver undergraduate and postgraduate cyber security education through a consistent curriculum and superior teaching. The profile of these centres will also help inspire students to think about careers in cyber security and study STEM subjects at school. The quality of graduates from the centres and the career opportunities available to them at home as well as abroad will also help influence up-and-coming students to seek career paths in Australia.

As well as university graduates with high-end cyber security skills, we need cyber security workers who can provide a range of functions to help organisations secure their networks. The Government will work with the private sector, the States and Territories and Skills Service Organisations to support the expansion of cyber security training in Registered Training Organisations (including TAFEs), potentially including the development of cyber security apprenticeships.

Australia's cyber security workforce also suffers from low participation from women— which means we are not harnessing the full potential of our talent pool. In worldwide terms, only 10 per cent of information security professionals are women. This too will be addressed through a range of integrated actions developed with the private sector and research community.

Expanding the national annual Cyber Security Challenge Australia from a focus on university students to a broader program of competitions and skills development opportunities for a wider set of participants, including those already in the workforce, will also help generate a sustained national pipeline of cyber security professionals. This includes competitions with other nations.

People at all levels in the workforce, including those in executive-level positions, will have the opportunity to improve their cyber security knowledge and skills by participating in short courses, executive training and other programs that supplement existing Master's courses with cyber security modules. This will also help increase the quality and quantity of people with cyber security skills.

RAISE NATIONAL CYBER SECURITY AWARENESS

Underpinning the success of all actions in this Strategy is addressing the comparatively low awareness of cyber security risks in the Australian community. Increasing the understanding of cyber security risks and benefits is one of our strongest defences, together with simple solutions to protect activities online. National behaviour change will ensure Australians are cyber security aware and protect themselves at home, school and work. By raising national cyber security awareness, Australians will protect themselves and others and feel more confident and willing to do business online.

A number of programs in Australian governments, the private sector and overseas have made some headway on improving cyber security awareness in Australian communities and around world. But a more sustained and coordinated effort is needed to achieve broader behavioural change.

The Government will partner with other Australian governments, businesses, researchers and community groups to deliver a sustained, national awareness-raising campaign, encompassing a range of activities, which enables all Australians to be secure online.

The program will seek to educate Australians on the real-world impacts of cyber risks and the way this affects our current and future prosperity.

We will also work closely with our international partners to coordinate awareness-raising activities regionally and globally, to complement capacity building efforts and increase the collective impact of messages.

07

ACTION PLAN

THIS ACTION PLAN
COMPLEMENTS THE STRATEGY
BY OUTLINING THE ACTIONS
THE GOVERNMENT WILL TAKE
TO ACHIEVE AUSTRALIA'S CYBER
SECURITY GOALS BY 2020

1. Governments, business and the research community together advance Australia's cyber security through a national cyber partnership.

2. Australia's networks and systems are hard to compromise and resilient to cyber attacks.

3. Australia promotes an open, free and secure cyberspace by taking global responsibility and exercising international influence.

4. Australian businesses grow and prosper through cyber security innovation.

5. Australians have the cyber security skills and knowledge to thrive in the digital age.

Recognising that cyberspace constantly changes, the Government will evaluate its progress and update this Action Plan annually.

A NATIONAL CYBER PARTNERSHIP

Goal: Governments, businesses and the research community together advance Australia's cyber security.

Action	Outcome
Deliver progress updates on the implementation of this Strategy	The Government evaluates its implementation progress and updates this Action Plan annually
Hold annual cyber security leaders' meetings	The Prime Minister and business leaders set the strategic cyber security agenda and drive the Cyber Security Strategy's implementation from the top-down
	Business leaders and the Government are equipped with the information they need to make appropriate investment and business decisions on their cyber security, including a collective understanding of emerging cyber challenges
Streamline the Government's cyber security governance and structures	Government responsibility for cyber security is well communicated and understood by stakeholders
	The Prime Minister appoints a Minister Assisting the Prime Minister on cyber security
	The Government's cyber security operations are coordinated, efficient and align with strategic priorities
	The Australian Cyber Security Centre is relocated to a facility that allows the Centre to grow and enables the Government and the private sector to work more effectively
Sponsor research to better understand the cost of malicious cyber activity to the Australian economy	A better understanding of the economic impact of cyber compromises to the Australian economy is developed
	Robust data is published that supports informed decision making on cyber security risk management and investment
	Robust data is published that improves the ability of organisations to consider the effectiveness of their investment in cyber security

STRONG CYBER DEFENCES

Goal: Australia's networks and systems are hard to compromise and resilient to cyber attack.

Action	Outcome
DETECT, DETER AND RESPOND	
In partnership with the private sector, establish a layered approach to cyber threat information sharing through: · partnerships between businesses and the Government within the Australian Cyber Security Centre; · co-designed joint cyber threat sharing centres (initially as a pilot) in key capital cities; and · a co-designed online information sharing portal	Partnerships between the Australian Cyber Security Centre and the private sector are increased and proven valuable for both parties An operating model for the joint cyber threat sharing centres is developed, successfully piloted and reviewed Based on the outcomes of the pilot, a rollout of joint cyber threat sharing centres nationally improves co-location of businesses, the research community together with State, Territory and Government agencies and share: · timely and actionable information on cyber security threats and risks; · knowledge about new/evolving actors and intrusion methods; and · expertise to solve problems and learn lessons from 'near misses' and compromises Cyber security information is delivered to a wider range of organisations through the online information sharing portal
Increase the Computer Emergency Response Team (CERT) Australia's capacity	CERT Australia's services are expanded for a wider group of businesses, with improved technical capability CERT Australia increases its international partnerships, focusing on prevention and shutting down malicious cyber activity
Boost the Government's capacity to fight cybercrime in the Australian Crime Commission	The Australian Crime Commission increases its capacity and capability to detect and analyse cybercrime
Boost the Government's capacity to fight cybercrime in the Australian Federal Police	The Australian Federal Police increases its capacity and capability to investigate cybercrime

Action	Outcome
Collaborate with Australian governments to ensure law enforcement officers receive the training they need to fight cybercrime across the nation	Skills needs for law enforcement officers, including specialist roles, to fight cybercrime are identified

A specialist training strategy is developed and implemented |
| Increase the Australian Signals Directorate's capacity to identify new and emerging cyber threats to our security and improve intrusion analysis capabilities | The Australian Signals Directorate increases its capacity and capability to identify cyber threats and develops responses to an increasingly complex digital environment

The Australian Signals Directorate expands the number of cyber security services it offers to a wider range of organisations |
| Strengthen Defence's cyber security capacity and capability, through initiatives in the 2016 Defence White Paper | Defence strengthens its cyber capabilities to protect itself and other critical Australian Government systems from malicious cyber intrusion and disruption

Defence enhances the resilience of networks, including networks used by deployed forces, and the capability of the Australian Cyber Security Centre and its cyber workforce, including new military and APS positions and training programs |
| Expand the nation's cyber incident management arrangements and exercises program | The Government's cyber incident management arrangements respond to the evolving cyber threat landscape

Australian governments understand how their respective cyber and incident response teams would operate together in a cyber crisis

The Government and private sector establish a program of joint cyber exercises

Australia works with international partners on developing policies for incident response as a confidence building measure |

Action	Outcome
RAISE THE BAR	
Co-design voluntary guidelines on good cyber security practice	The Government and private sector co-design and publish baseline guidance for Australian cyber security that provides a benchmark for good practice, informs cyber security insurance and meets corporate obligations
	Australia's good practice guidelines are an economic and security asset—they provide a commercial advantage and ensure cyber risks to critical services are risk assessed and managed
	Australian businesses, small and large, have improved understanding of good cyber security practices
	Governments, critical services and high risk sectors demonstrate good cyber security practices
Continue to regularly update the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions	The Strategies to Mitigate Cyber Intrusions remain world leading publicly available advice on how to best protect against targeted malicious cyber activity
Co-design voluntary cyber security 'health checks' for ASX100 listed businesses	Executives and boards in the ASX100 better understand cyber security strengths and opportunities for their business
	Decision makers in the ASX100 receive tailored information on the impact of cyber risks to their companies
	Australia's highest performing businesses lead a national effort towards best practice cyber security
	Increased cyber resilience in Australia's largest companies
Support the Council of Registered Ethical Security Testers (CREST) Australia New Zealand to expand its range of cyber security services	CREST Australia New Zealand grows its current pool of accredited companies to meet the demand of businesses accessing their services
	CREST Australia New Zealand diversifies the services it accredits. Types of assessment might include penetration testing, vulnerability analysis and assessment against best practice standards

Action	Outcome
Support small businesses to have their cyber security tested by CREST Australia New Zealand accredited providers	Australian small businesses have access to accredited experts to assess their cyber security, helping them to take responsibility for the security of their own networks
	Australian small businesses understand their potential cyber security vulnerabilities and where to find trusted cyber security advice
	Australian small businesses are empowered with the knowledge they need to make considered cyber security investments to protect their business long term
	Large and small businesses increase trust in the connections they have with each other
Improve Government agencies' cyber security through a rolling program of independent assessments of agencies' implementation of the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions	Government agency cyber security practices are the exemplar for public and private sector organisations in Australia
	Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability
	Non Government information stored on Government networks is resilient to malicious cyber activity
Improve Government agencies' cyber security through independent cyber security assessments for agencies at higher risk of malicious cyber activity that also helps those agencies address the findings	Government agency cyber security practices are the exemplar for public and private sector organisations in Australia
	Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability
	Non Government information stored on Government networks is resilient to malicious cyber activity
Improve Government agencies' cyber security through increasing the Australian Signals Directorate's capacity to assess Government agencies' vulnerability, provide technical security advice and investigate emerging technologies	Government agency cyber security practices are the exemplar for public and private sector organisations in Australia
	Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability
	Non Government information stored on Government networks is resilient to malicious cyber activity
Develop guidance for Government agencies to consistently manage supply chain security risks for ICT equipment and services	Government agencies have clear guidance on identifying and managing cyber security risks when procuring ICT equipment and services

GLOBAL RESPONSIBILITY AND INFLUENCE

Goal: Australia actively promotes an open, free and secure cyberspace.

Action	Outcome
Appoint a Cyber Ambassador	Australia has a coordinated, consistent and influential voice on international cyber issues
Publish an international engagement strategy on cyber security	Australia's international engagement on cyber issues is prioritised and coordinated Stakeholders understand Australia's position on key cyber issues being debated on the world stage
Champion an open, free and secure Internet to enable all countries to generate growth and opportunity online	Australia actively participates in key international cyber fora to promote agreed peacetime norms of appropriate state behaviour in cyberspace
Partner internationally to shut down safe havens and prevent malicious cyber activity, with a particular focus on the Indo-Pacific region	Australia's relationships with a broad range of international counterparts on operational cybercrime collaboration are strengthened International efforts to prosecute cybercrime are enhanced
Build cyber capacity in the Indo-Pacific region and globally, including through public-private partnerships	Cyber capacity in the Indo-Pacific region, including through partnerships with businesses and the research community, is increased and contributes to improved cyber maturity

GROWTH AND INNOVATION

Goal: Australian businesses grow and prosper through cyber security innovation.

Action	Outcome
Establish a Cyber Security Growth Centre to bring together a national cyber security innovation network that pioneers cutting edge cyber security research and innovation, through the National Innovation and Science Agenda	Connections made between stakeholders, through the Growth Centre, deliver a multiplier effect on cyber security ideas and the number of challenges being responded to increases More cyber security start-ups acquire capital to establish More cyber security solutions are developed and commercialised The number of cyber security businesses in Australia grows More Australian cyber security products and services are exported More international businesses invest in Australian cyber security research, innovation and solutions All businesses benefit from cyber security solutions commercialised with Growth Centre support
Boost Data61's capacity for cyber security research, support to commercialisation of cyber security solutions, improving cyber security skills and deepening connections with international partners, through the National Innovation and Science Agenda	Data61's efforts on cyber security research and innovation have a multiplier effect on the activities within the Growth Centre's national cyber security innovation network The number of students in cyber security PhD programs increase, through the support of Data61 scholarship programs SINET is successfully established in Australia bringing together cyber innovators, buyers and investors, complementing activities of the Cyber Security Growth Centre
Work with business and the research community to better target cyber security research to Australia's cyber security challenges	Australia's cyber security R&D is robust, competitive and coordinated Australia's cyber security R&D explores current and emerging challenges for Australia's national cyber security
Promote Australian cyber security products and services for development and export	The Australian public and private sectors mature their understanding of home-grown cyber security capabilities The Government invests in developing Australian-based cyber security ideas More international organisations invest in Australia and the Australian cyber security sector

A CYBER SMART NATION

Goal: Australians have the cyber security skills and knowledge to thrive in the digital age.

Action	Outcome
Partner with Australian governments, businesses, education providers and the research community in a national effort to develop cyber security skills to: • establish academic centres of cyber security excellence in universities; • ensure qualifications in the ICT field provide cyber security skills; • introduce programs for all people at all levels in the workforce to improve their cyber security skills and knowledge, starting with those in executive-level positions; • continue to raise awareness in schools of the core skills needed for a career in cyber security; • understand and address the causes of low participation by women in cyber security careers; and • expand the Government's annual Cyber Security Challenge Australia to a broader program of competitions and skills development.	The skills of university graduates and technical college students with cyber security qualifications are improved The number of cyber security graduates increases The number of children studying subjects at school that will equip them for careers in cyber security increases More women and people with diverse backgrounds take up and change to a career in cyber security People at all levels in the workforce, including those in executive-level positions, have the opportunity to improve their cyber security knowledge and skills by participating in competitions, short courses, executive training and other programs such as Masters degrees Opportunities to participate in Australian cyber security competitions increases, including internationally
Bring together and grow public and private sector cyber security awareness programs to make the best use of combined resources	More people have improved knowledge of the real-world impacts of cyber risks and the way they affect our current and future prosperity
Work with other countries on cyber security-awareness-raising programs to deliver mutually beneficial outcomes	We achieve economies of scale through joined-up awareness-raising programs

Australian Government