# AUSTRALIA'S CYBER SECURITY STRATEGY

Enabling innovation, growth & prosperity

## FIRST ANNUAL UPDATE 2017

Australian Government

**Australia's Cyber Security Strategy: 2017 Update**
© Commonwealth of Australia 2017

ISBN 978-1-925362-45-9 Australia's Cyber Security Strategy: 2017 Update (PDF)
ISBN 978-1-925362-46-6 Australia's Cyber Security Strategy: 2017 Update (HTML)

# TABLE OF CONTENTS

# PRIME MINISTER'S FOREWORD

The Hon Malcolm Turnbull MP
Prime Minister

2017 is a turning point for cyber security in Australia. One year on, my Government's landmark Cyber Security Strategy has been a catalyst for change.

The conversation has shifted – in government, in business and for individuals. Trust and confidence through cyber security is becoming economic and security currency for Australia. And while the speed of change has been remarkable, much more is to come. No Australian government has ever been more committed to protect our interests in cyberspace.

The Cyber Security Strategy has generated momentum. It has encouraged the private sector to incubate ideas and initiatives well beyond those outlined the Strategy. Success is not just ticking off the Strategy's initiatives, but changing culture. Enhancing trust and confidence in the confidentiality, integrity and availability of networks and data will help us derive even greater economic value from information-driven change.

Our initiatives have had a clear impact. The cooperation between government and business is stronger and deeper; boardrooms and Commonwealth agency heads are more attuned to cyber risks. State and territory governments are engaged; and the tempo of international engagement is quickening.

My Government's new appointments - Minister Assisting the Prime Minister for Cyber Security, Special Adviser to the Prime Minister on Cyber Security, Ambassador for Cyber Affairs – have led the way, shaping a new cyber security agenda. The Australian Cyber Security Growth Network has hit the ground running, providing a platform to unearth innovative cyber companies and help them grow. Attracting more talent – in particular more women – into the profession is a priority.

And as a result, culture is beginning to change. But change has been faster in the private sector than in government. The Minister Assisting the Prime Minister for Cyber Security and Special Adviser to the Prime Minister on Cyber Security help me provide the voice of leadership to the government cyber security community, and have my backing to challenge agencies to be more agile and accelerate our progress.

Australia will face major cyber security challenges in the future. Australian families and businesses continue to be targeted by cybercriminals. Some foreign nations continue efforts to compromise our national security. Over the past year we have witnessed cyber security events here and overseas disrupt infrastructure and services, cause hundreds of millions of dollars in damage to companies, threaten the confidentiality of networks on an unprecedented scale, and attempt to interfere with democratic processes. This is unacceptable.

It is time therefore to capitalise on the vision set out in the Cyber Security Strategy. We will build even greater collaboration between government and the private sector, stimulate further innovation, and develop new paradigms for countering cyber security challenges for a more secure and prosperous Australia.

# MINISTER ASSISTING THE PRIME MINISTER FOR CYBER SECURITY FOREWORD

The Hon Dan Tehan MP
Minister Assisting the Prime Minister for Cyber Security

Australia's Cyber Security Strategy - the first fully funded and comprehensive plan for Australia's cyber security - is critical for our nation's security and prosperity.

The four-year strategy is only a year old and we have already made great strides. The Government has delivered on many initiatives, and set Australia on the path for the successful delivery of others.

We have opened the first Joint Cyber Security Centre in Brisbane which is the first stage of a $47 million program piloting collaborative work spaces where industry, government and law enforcement work together and share relevant threat information. We are accelerating our plans to launch more centres in other capital cities.

The Australian Cyber Security Growth Network has been established with $31.9 million in funding from 2016-17 to 2019-20 to ensure Australian businesses can take advantage of opportunities in the global cyber security industry.

The Turnbull Government has committed a further $3.45 million to help address Australia's shortage of skilled cyber security professionals via the establishment of Academic Centres of Cyber Security Excellence. The centres will produce work-ready graduates to increase our cyber security workforce and world-leading research on cyber security as well providing executive education programs for industry and government.

Work will begin later this year delivering the Government's $38.8 million fitout and relocation of the Australian Cyber Security Centre to Brindabella Park in Canberra. The new centre will be home to the Government's cyber agencies as well as representatives from across the private sector.  The new multi-classified space will allow business and academia to more easily work side-by-side with government to share information and counter cyber security threats.

The recent development in statecraft of using cyber to attempt to influence the democratic process required a government response. Prime Minister Turnbull was quick to arrange a briefing of all political parties on strengthening cyber security. Australians must have confidence that when they cast their vote they are taking part in a strong, robust democratic process that is built for the modern world.

The Government also recognises we cannot ensure Australia's cyber security alone. Governments, business and individuals must work together to share information and strengthen our defences against cyber threats.

The private sector has an important role to play because it is the driver of growth, employment and innovation. And the initiatives delivered through the cyber strategy have been designed to encourage and facilitate cooperation between government and business and, just as importantly, between business and business.

The Government-backed ASX 100 Cyber Health Check of Australia's leading businesses will provide a valuable snapshot of the understanding of the cyber landscape. These checks are a key initiative under the Cyber Security Strategy, which will increase the cyber resilience in Australia's largest companies through raising awareness and enabling ASX 100 companies to better understand their cyber security risks and opportunities.

In the world of cyber security, if you are standing still you are going backwards. The cyber security environment is constantly evolving, and we need to be adaptive and proactive. This update also captures work that has been done in addition to the Cyber Security Strategy, as well as identifying next steps and new work to be pursued. Ensuring the Australian Government's strategy for cyber security is not static will ensure we can be confident in facing the cyber security challenges on the horizon.

Moving forward, we must concentrate on ensuring the cyber security of individuals, small and medium sized businesses and our critical infrastructure.

We are putting more digital cops on the beat and we will be working closely with our partners to understand how to better counter cybercriminal activity targeting small business and families.

We need to work with businesses and state and territory governments to better secure our critical infrastructure. This will involve better coordination and potentially reform of legislation.

This Government recognises the importance of strong cyber security to our nation and we will continue to increase our efforts to work collaboratively with industry, academia and individuals to keep all Australians safe online.

# EXECUTIVE SUMMARY

The last twelve months have been seminal in shaping the security of Australia's online future.  Australia's four-year Cyber Security Strategy is delivering on the Government's promise of improving the security of Australia's online environment, and enabling innovation, growth and prosperity. Strong progress has been made against the Cyber Security Strategy's 33 initiatives, with several delivered and others well in train.

But even more, the Cyber Security Strategy has generated momentum and established a platform for more direct, deeper and richer conversations between governments, business and the public. As custodians of the economy and the providers of our online infrastructure, the private sector plays the central role in Australia's cyber security. Success requires a true partnership.

> *"The Cyber Security Strategy has brought a coordinated focus to cyber security. It has started conversations; now the focus must be on delivering each of the initiatives identified under the strategy and we would like to see this being accelerated as the fast moving threat environment requires increased agility".*
> *- Berin Lautenbach,*
> *Acting Chief Information Security Officer, Telstra*

2017-18 is shaping as another pivotal period for Australia's cyber security. The platform set by the Cyber Security Strategy presents a unique opportunity for Australian businesses and government agencies to seize the initiative and drive towards bigger and better goals. This update outlines some of those, and more will emerge over the next twelve months.

The Government, through the Office of the Cyber Security Special Adviser, will lead new areas of work focusing on tackling cybercrime, supporting small business, securing critical infrastructure and building cyber resilience. We will disrupt the Strategy where necessary, continue to improve communications, be more agile and accelerate the implementation of key initiatives.

# Cyber Landscape – One Year On

Australia's Cyber Security Strategy has generated a vibrant discussion about cyber security as a key element of national prosperity and security. Cyber security has been recognised as an enabler not only to improve existing ways of doing business, but as a critical new industry that can drive Australia's future prosperity. For Australia to be globally competitive, cyber security must underpin the data-driven transition of every sector in the economy.

The need to deal with cyber security challenges has never been better understood. Boards recognise it as a key business risk, and also a competitive edge; Commonwealth, state and territory governments better understand its importance for national security, prosperity, and improving the lives of all Australians.

Key to Australia's future prosperity is a strong and vibrant online economy. Growth of our cyber security businesses, support to innovation and active collaboration between our research and business sectors is critical for achieving leadership and a reputation for trust in the global economy. The Cyber Security Strategy provides an overarching, organising framework for all Australian businesses to grow and prosper through cyber security innovation.

> *"There's a buzz and an energy around the Australian cyber security industry that is unlike anything we've had before." **Nick Ellsmore, Security Advisor & Chief Apiarist, HIVINT***

Since the launch of the Cyber Security Strategy we have seen a rapid growth in interest, energy and focus across the cyber security sector. The activity across the Australian economy has outstripped expectation. Australia ranks fourth globally in patent filings in cyber security research and development. Not only have the initiatives under the Cyber Security Strategy had a direct effect, but industry, academia and government agencies have increased their rate of engagement on cyber security. This is growing into a thriving community that will help protect Australia's economy and continue to grow into a valuable and profitable industry sector.

If Australia invests further in cyber security, it would unlock potentially valuable investments in digital innovation, boosting most businesses. According to Deloitte, by 2030 this could lead to:

- A lift of 5.5% in business investment;
- Wages up 2.0%;
- An extra 60,000 people employed, and Australia taking its share of a likely booming Indo-Pacific cyber security market.

Australians are embracing the Internet for business and personal use more than ever before.

- In the second half of 2016, the volume of data downloaded through broadband connections was 23% greater than the first half of 2016, continuing a long-term trend of growing Internet usage.
- In June 2016, 94% of adult Australians used the Internet to conduct banking, pay bills, or buy and/or sell goods and services.

While Australian companies are being hit with more malicious cyber activity, they are putting in place better means to deal with it.

- In 2016, 59% of organisations in Australia detected a business interrupting security breach on at least a monthly basis, which is more than twice as often as 2015, according to the 'Telstra Cyber Security Report 2017'.
- 71% of respondents to the ACSC 2016 Cyber Security Survey reported having a cyber security incident response plan in place, compared to 60% in 2015.
- According to the 'ACSC 2016 Cyber Security Survey Report', organisations with higher levels of cyber resilience were more likely to have discussed cyber security at the board level in the past three months.
- 39% of CIOs had purchased some form of cyber insurance in 2016, compared to 24% in 2015, according to the Minter Ellison 'Perspectives on Cyber Risk 2017' report.

## 2016 – CYBER SECURITY EVENTS SHAPING AWARENESS

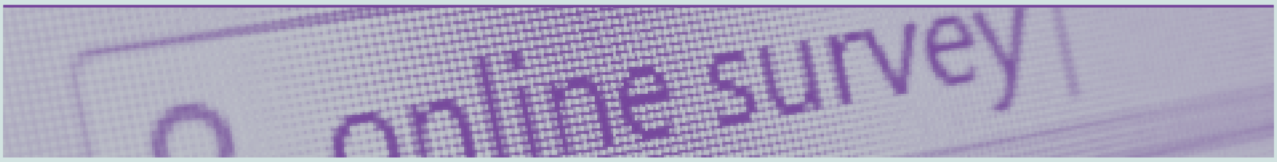
### US ELECTION INTERFERENCE

The hack and release of sensitive information from the US Democratic National Committee by Russian cyber actors in the lead up to the 2016 US Presidential election demonstrated how targeted disclosures of stolen information can interfere with processes underpinning Western democracy. The interference broke new ground for unacceptable behaviour and tested concepts around public attribution, response and effective deterrence. It also encouraged discussion over the security of electoral systems, including on-line voting.

### INTERNET OF THINGS CYBER ATTACKS

The unprecedented scale of the Distributed Denial of Service attack on US Domain Name System provider Dyn disrupted major internet platforms and services in North America, Europe and Australia. The Dyn disruption was enabled by the exploitation of security vulnerabilities in Internet of Things devices – including closed-circuit television equipment – and gave cause to consider critical dependencies and vulnerabilities in Australia's Internet infrastructure, and the security of Internet-connected devices.

### eCensus



Overnight Australians – and the Government – understood the devastating effect cyber security can have on trust as the hashtag #Censusfail trended globally. The incident tested confidence in government's digital transformation agenda and online service delivery more broadly.

### DATA BREACHES

Multiple public breaches of sensitive data by Australian companies and government entities raised privacy concerns. Most of these were not due to network compromises, but the result of complacency and failures in the delivery and management of ICT services and information. In October, sensitive personal information of 550,000 customers of the Australian Red Cross Blood Service was exposed online through human error. While there was no discernible impact or threat to donors following the incident, the Red Cross' swift and proactive response – engaging the Australian Cyber Security Centre, and establishing a support service for affected persons – was critical to mitigating the harm.

Government is assisting through the Computer Emergency Response Team (CERT) Australia. Over the past year CERT Australia:

- published 159 advice reports covering topics such as critical vulnerabilities in industrial control and building management systems, as well as malicious activity targeting banking applications; and
- handled 10,351 incidents affecting businesses, of which 363 were more serious incidents affecting systems of national interest.

The Australian Cyber Security Centre 2016 Threat Report showed how the landscape of cyber security threats and challenges affecting Australia continues to evolve (see also text box). Notable events in 2016 and 2017 expanded Australians' awareness of how cyber security can impact our lives. Public expectations for improved privacy, integrity and availability of online services will only increase. Government and business will need to be better at anticipating and responding to future cyber security challenges to prevent shocks.

Cybercrime remains the most visible and damaging aspect of the cyber threat environment for the majority of Australian citizens and businesses. Almost all Australians that use the Internet are exposed to sophisticated cybercriminals seeking to steal money. Or to steal information or threaten to disrupt services for the purposes of fraud and extortion.

## CYBERCRIME – MORE OF IT, MORE SOPHISTICATED, AND MORE TARGETED AGAINST AUSTRALIANS

The Australian Criminal Intelligence Commission has built a stronger picture of the identities and methodologies of cybercriminals targeting Australia – mostly originating from Eastern Europe and Russia. This includes a class of offshore cybercriminal that specialise in targeting Australians.

The proliferation of ransomware – where the victim is prevented from accessing their systems or data until a ransom is paid – remains an endemic problem across the globe. In Australia, reports of ransomware activity reported to the Australian Cybercrime Online Reporting Network roughly doubled in 2016 compared to 2015.

Australia remains the main target of malicious software – predominantly ransomware and software that steals personal information – in the Asia Pacific region in 2016, likely due to our economic prosperity and high adoption of technology.

# A National Cyber Partnership

## GOAL

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

The Cyber Security Strategy has created energy and a new dynamic of collaboration between the public and private sectors and academia. Leaders are setting the tone that this is an issue of opportunity as much as threat.

## DELIVERING THE STRATEGY

- The Prime Minister continued to host annual cyber security leaders' meetings. The April 2017 conversation canvassed technological advances that will potentially disrupt Australia's cyber security ecosystem and strategies to get ahead.
- The Government's new lines of cyber security authority – Minister Assisting the Prime Minister for Cyber Security, Special Adviser to the Prime Minister on Cyber Security, Ambassador for Cyber Affairs and Coordinator Australian Cyber Security Centre – are already delivering benefits in terms of leadership and improved strategic consultations.
- New governance arrangements have been implemented to focus effort within government, including transition of strategic leadership to a new Cyber Security Board chaired by the Secretary, Department of the Prime Minister and Cabinet.
- Following a recommendation by the Public Works Committee, the Australian Parliament has passed a motion to expedite the relocation of the Australian Cyber Security Centre to Brindabella Business Park in Canberra. Ongoing cultural change in the Centre along with successful relocation should increase the opportunity for strong public-private collaboration.
- The Office of the Cyber Security Special Adviser has commenced initial scoping to deliver research to better understand the cost of malicious cyber activity to the Australian economy. Work will be progressed in collaboration with the private sector across 2017-2018.

> *"We are seeing the strategy provide a valuable platform for increased industry and government collaboration, and facilitating information exchange between big and small businesses to keep our collective employee base, our customers, and the community safe."*
> *Andrew Dell, Chief Information Security Officer, National Australia Bank*

## BUILDING ON THE STRATEGY

Strengthening Commonwealth, state and territory engagement on cyber issues, the Prime Minister led a discussion on current and emerging cyber risks at the December 2016 Council of Australian Governments meeting. Leaders noted cooperation to date and agreed to improve collaboration to manage cyber security risks and strengthen public trust and confidence in Australia's online economy. Identified areas of future cooperation included critical infrastructure resilience, cyber incident management response, and cyber security education. These discussions have been backed up by regular dialogue between officials.

The Minister Assisting the Prime Minister for Cyber Security has actively engaged the private sector on cyber security, hosting quarterly dialogues with industry. Recent dialogues have focused on cyber security incident response and uplifting the cyber security capacity in small to medium enterprises

Across the economy, Boards have been seeking further information about cyber security risks and opportunities; in government cyber security has been regularly discussed at the Secretaries' Board, which brings together the Secretaries of all Commonwealth Departments and is Chaired by the Secretary of Prime Minister and Cabinet; and the Special Adviser to the Prime Minister on Cyber Security has also briefed Commonwealth Parliamentarians and several state and territory governments on cyber security risk.

## NEXT STEPS

2017 will see the relocation of the Australian Cyber Security Centre to Brindabella Business Park in Canberra. This move will bring the policy and operational elements of government closer together, and provide more opportunities for meaningful collaboration with the private sector at a variety of security classification levels.

While an uptick in communications and engagement by government has raised awareness, it is clear that more can be done to communicate the integration of the initiatives within the Cyber Security Strategy, including who does what in government. Responding to that feedback, the Government, through the Office of the Cyber Security Special Adviser, will publish a view of the cyber security ecosystem and the Government's cyber security governance arrangements, and mature its communications channels to provide more regular progress updates.

The Government, through the Office of the Cyber Security Special Adviser, will also seek to bring more diverse views and expertise into the development of cyber security policy, in effect "crowd sourcing" the identification of issues, priorities and options.

> *"The Australian Government recognises that cyber security is not a job that government can do alone. Technology connects us all and provides us with unheralded opportunities for innovation and profit, but it also unites us in a shared vulnerability."*
> *The Hon Dan Tehan MP, Minister Assisting the Prime Minister for Cyber Security*

# Strong Cyber Defences

# GOAL

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

By strengthening our cyber defences, we build resilience and derive trust and confidence. Cyber security incidents also offer an opportunity to learn. We continue to share and collaborate between the public and private sectors, but we need to change the parameters and be more forward leaning: getting Joint Cyber Security Centres up and running is just the beginning.

## DELIVERING THE STRATEGY

- The pilot Joint Cyber Security Centre was opened in Brisbane on 24 February 2017. More than 20 organisations are represented from the energy, water, finance, transport and mining sectors, as well as Queensland Government, CERT Australia, the Australian Federal Police and the Australian Criminal Intelligence Commission. Priorities for the Centre are automated information sharing and targeted analysis of specific cybercrime threats against Australian industry networks.

- CERT Australia has commenced scoping the Cyber Security Information Sharing Portal, building on their existing industry portal and the Australian Signals Directorate's OnSecure service for government agencies.

- Government's cyber security agencies have been recruiting: CERT Australia has expanded its capability to provide specialised security advice to Australia's critical infrastructure companies on industrial control systems; the Australian Criminal Intelligence Commission has boosted its capacity to link online cybercrime personas with real world identities, pinpointing a group that specialise in targeting Australians.

- The Australian Federal Police has commenced a comprehensive program to up-skill staff to tackle contemporary cybercrime. Programs for cyber investigators are also open to participation by state and territory police.

- The Office of the Cyber Security Special Adviser has comprehensively revised the Government's Cyber Incident Management Arrangements which outline roles and responsibilities for response to malicious cyber incidents. The arrangements are being tested with the private sector in April 2017.

> *"Crisis incident response remains a key challenge across government and business given the uncertainty and intangible nature of cyber incidents compared to other incidents such as natural disasters and terrorism. A joint program between government and the private sector is important so that capability and best practices can be shared".*
> ***Steve Jackson, Head of Security, Qantas***

- CERT Australia has drafted national cyber security exercise program guidelines and an evaluation framework, which will be socialised with Commonwealth, state and territory governments and private sector partners. Two discussion exercises have been held and a program is being developed to test a range of cyber readiness and resilience scenarios.

- The Australian Signals Directorate's Strategies to Mitigate Cyber Security Incidents has been comprehensively updated. A new Essential Eight sets a contemporary global cyber security standard, with practical steps organisations can implement to make their networks and data more secure.

- A public-private co-design process, led by CERT Australia, kick-started the development of Voluntary Cyber Security Guidelines in late 2016.

- The Department of Defence has commenced recruitment and capability planning for the cyber security initiatives to be delivered through the Defence White Paper 2016.

- The ASX 100 Health Check has brought cyber security into our top boardrooms, with an April launch of the industry-led survey report on cyber security governance in our top companies.

- The Australian Signals Directorate conducted surveys of Commonwealth agencies' cyber security postures based on their implementation of the 'Top 4' Strategies to Mitigate Targeted Cyber Security Incidents (from 2017, this will extend to the 'Essential Eight'). This effort allows the Commonwealth to focus security efforts on high risk agencies and systems of national importance.

## BUILDING ON THE STRATEGY

The #Censusfail of 2016 afforded Government an opportunity to look introspectively at how cyber security is implemented. From system design to contract management, there were lessons for all government agencies. As a result, we will see greater awareness of cyber security at the executive level, increased understanding and uptake of cloud services, and the security of online systems being assessed with more rigour – ensuring the Australian public trust the government to deliver securely online.

Following the declaration of Australia's offensive cyber capability in the Cyber Security Strategy, the Prime Minister announced in November 2016 that offensive cyber capabilities are being employed in support of Australian Defence Force operations against Islamic State. This contributes to our national deterrence posture, and promoted mature discussion about the application of such capabilities under international law.

The Australian Cyber Security Centre 2016 Threat Report - the most forward leaning yet in describing government's understanding of the cyber security landscape - was welcomed by the private sector for its content and practical guidance on cyber security mitigation. Delivering on the Prime Minister's intent to be more open about acknowledging, explaining and analysing the problem, the Government is committed to continuing to publish material in this vein, such as the April 2017 advice on the global targeting of enterprises via malicious compromise of managed service providers.

The Australian National Audit Office continued its program auditing the cyber security posture of government agencies.

## NEXT STEPS

Australians and their businesses are at the front line of cybercrime and they expect government to act. The Government is committed to working with states and territories to enhance our national response, including through a proposal to develop a new 'National Plan to Combat Cybercrime'. Working with industry, government will also explore a policy framework to identify measures to protect Australians from cybercrime: more than merely logging and monitoring malicious activity, to take proactive steps to reduce the threat.

The new Critical Infrastructure Centre in the Attorney-General's Department – in cooperation with the Australian Cyber Security Centre – will work closely with our national critical infrastructure companies to identify cyber vulnerabilities, develop risk assessments and risk management strategies.

The Joint Cyber Security Centre program will be accelerated to meet demand with further centres to open in Melbourne, Sydney and Perth in 2017. This will be followed by Adelaide in the first half of 2018 and this will ensure that we have more on the ground exchange of information and expertise, more quickly.

It has become clear since the launch of the Cyber Security Strategy that more needs to be done to support the cyber security capacity of Australia's small and medium businesses. Consultation has commenced with both small and large businesses and industry associations about developing a targeted approach. Initiatives will take account of the reality of the environment in which these businesses operate, where time and resources are not readily available to tackle what can seem to be an insurmountable problem. This will complement the Cyber Security Strategy commitment to expand the services of the Council of Registered Ethical Security and Testers Australia and New Zealand and provide grants to small business to access these services, which will commence in 2018.

Work will commence on scoping a policy approach to ICT supply chain security risks to government systems and services. Government will also collaborate with industry to identify practical measures to improve the security of Internet of Things devices.

> *"The Strategy has helped raise the profile of the risks of cyber attack for the 3 million small to medium enterprises in Australia but more needs to be done. Many small businesses don't understand customer databases are valuable and ransomware can bring most businesses to a standstill. The challenge for the next 12 months is to show all businesses that they are easy targets if they have not adopted simple and inexpensive procedures to protect their data and systems."*
> *Kate Carnell, Australian Small Business and Family Enterprise Ombudsman*

# Global Responsibility and Influence

# GOAL

Australia actively promotes an open, free and secure cyberspace.

The Prime Minister and the Minister Assisting the Prime Minister have led international collaboration on cyber security. The Ambassador for Cyber Affairs has hit the ground running. Engagement throughout the region has grown and an international engagement strategy will sharpen our focus. Creative partnering arrangements with the private sector will increase our efficiency and broaden our reach.

## DELIVERING THE STRATEGY

- Dr Tobias Feakin was appointed Ambassador for Cyber Affairs and has already become an influential voice on the world stage. Signalling the Government's priorities, his initial visits included Singapore, Malaysia and Indonesia.
- Following a public consultation process, Australia's first international cyber engagement strategy is on-track for release in 2017. By identifying priorities for engagement and communicating goals to the Australian community our engagement and capacity building efforts will be better coordinated and hence more efficient and effective.
- Australia has continued its advocacy for an open and free Internet, including through its position on the United Nations Group of Government Experts, ASEAN Regional Forum, International Telecommunication Union, Freedom Online Coalition, G20, and direct bilateral engagement.
- Partnering with the UN Office on Drugs and Crime, Australia supported a cybercrime training program in Bangkok in October 2016. Cyber workshops and training programs have been held with other nations, such as Papua New Guinea, Vietnam and Indonesia.
- The Australian Federal Police has also delivered a variety of cyber training through its extensive liaison officer network to upskill Australia's law enforcement partners. This work has been accompanied by the establishment of dedicated Australian Federal Police Cybercrime Liaison Officers and Australian Criminal Intelligence Commission cybercrime analysts in Washington DC and London.
- The Department of Foreign Affairs and Trade launched first-round funding of public-private cyber capacity building projects under its Cyber Capacity Program.

## BUILDING ON THE STRATEGY

Together with business leaders, the Government held the first joint public-private sector Australia and United States cyber security dialogue which was headlined by the Australian Prime Minister. A similar dialogue has also been initiated with Israel. Through these mechanisms Australia can model global responsibility and champion the values of an open, free and secure Internet.

The Ambassador for Cyber Affairs is increasing Australia's influence and ensuring our core national values – freedom of speech, rule of law and the right to privacy – are central to the global cyber affairs debate.  Defending the international rules based order and influencing emerging norms of state behaviour in cyberspace to be consistent with Australia's core national values is a long-term project. A project made all the more important by the tumultuous and unpredicted global events that have punctuated the Strategy's first year.

Australia has continued cyber policy dialogues with China, India, South Korea, Japan, New Zealand and will shortly hold its inaugural dialogue with Indonesia. In February 2017, cyber security was permanently added to the agenda of the Australia-Indonesia Ministerial Council on Law and Security. Bilateral cyber policy engagement has been expanded with other Indo-Pacific nations, including Singapore, Fiji and Samoa.

Australia is also alive to its obligations in the region. CERT Australia is delivering on its commitment to the regional CERT community through its leadership of the Asia Pacific CERT, and increased involvement in Asia-Pacific capacity building. Australia is also embracing a future where a flourishing private sector works in parallel to formal diplomacy to organically advocate our values and spread necessary cyber security skills and products throughout the region. To that end, Austrade is refining its outreach work and maximising trade opportunities for Australian cyber security businesses.

International collaboration is about more than law and values. Australia is leading collaboration between international partners and like-minded countries on incident management, with expansion of international exercising having included New Zealand.

> *"Australia's international cyber strategy and the effective engagement of the private sector will have important ramifications for Australia and the Asia Pacific region."*
> ***Steve Jackson, Head of Security, Qantas***

## NEXT STEPS

Australia's international cyber engagement strategy will both prioritise our international cyber security goals and communicate that agenda to the community. Optimised engagement efforts, combined with the delivery of a rolling series of capacity building grants, will accelerate collaborative partnerships with regional nations. Australian know-how will boost cyber security skills and governance in our region. Further iterations of dialogues with business will continue to strengthen public-private sector cooperation and further engage the private sector on addressing threats and realising the opportunities of the Internet.

# Growth and Innovation

## GOAL

Australian businesses grow and prosper through cyber security innovation.

The Australian Cyber Security Growth Network is on the verge of shifting the cyber security ecosystem. Government's research capabilities will line up behind industry's priorities as identified by the Growth Network. Talented and innovative cyber security companies are being unearthed and first steps have been taken to attract venture capital and access global cyber security markets.

> *"Creating a vibrant cyber security industry in Australia will deliver a measurable economic benefit to this country through jobs and new business opportunities."*
> *Craig Davies, Chief Executive Officer*
> *Australian Cyber Security Growth Network*

## DELIVERING THE STRATEGY

- The Australian Cyber Security Growth Network commenced operations in early 2017 and has been the catalyst for new energy in the cyber security start up and scale up sector. Negotiations have been finalised for the first two network nodes and the Growth Network is in active engagement with other jurisdictions for announcements later in 2017.
- The Growth Network has already begun taking Australian cyber security products and services to the world – starting with a highly successful delegation to the RSA Conference in San Francisco.
- Government's data innovation capability, Data61, has been actively driving new opportunities to bring Australia's cybersecurity ecosystem together and encourage information sharing, cross-collaboration and growth across Australia's cyber security research, government and industry cohorts. Data61 has been crucial in supporting the early activities of the Growth Network, and establishing SINET61 - the partnership between Data61 and the SINET international network of cyber security professionals that brings together venture capital and innovators.
- Over 40 of Data61's PhD students have a specific focus on cyber security related themes and this number is expected to continue to grow significantly in 2017. Data61's current scholarship round includes twelve new cyber focused PhD offers.

## BUILDING ON THE STRATEGY

The Department of Industry, Innovation and Science is upskilling its Entrepreneurs' Programme Business Advisers to recognise businesses facing a high cyber threat environment and provide advice around cyber resilience, information security and cyber security maturity. This will directly support Australian small and medium enterprises.

In February, Austrade delivered a comprehensive program of events, briefings, and site visits for 26 Australian cyber security companies, as part of the Cyber Security Mission to the San Francisco Bay Area, coinciding with the world's largest cyber security conference, RSA 2017. The newly appointed CEO of the Australian Cyber Security Growth Network led the mission, which provided the delegation with an opportunity to connect with potential partners, customers, and investors.

Austrade also released its Cyber Security Industry Capability Report, highlighting Australia's strengths and capabilities both in home grown industry and as a location for international investment in cyber security. International companies have taken note of the Cyber Security Strategy's direction and have chosen to invest in Australia. Austrade's program of landing pads also provides a safe location for Australian cyber security business to access global opportunities. SINET61 has also provided access to global institutional investors specialising in cyber security via the SINET61 network.

Domestically, partnering arrangements between industry and our academic institutions is growing, strengthening research, innovation and skills development. Examples include the Oceania Cyber Security Centre, which brings together eight Victorian universities as well as the Defence Science Institute and private sector organisations, and initiatives between Optus and Macquarie University; the Commonwealth Bank and the University of New South Wales;  Dimension Data and Deakin University; and CISCO and Edith Cowan University, the University of New South Wales and Curtin University.

> *"As an innovative, growing cyber-security company, we see the focus on bringing businesses and researchers together to develop the next generation of products and services as highly encouraging for the future of our indigenous cyber-security capability."*
> *Dr Jane Melia, Vice President of Strategic Business Development, QuintessenceLabs*

Through its Next Generation Technologies Fund, the Department of Defence has invested in a partnership between Data61 and several Australian universities to drive strategic research and development into tackling emerging threats to Australia's cyber security.

# NEXT STEPS

The Australian Cyber Security Growth Network plans a further two international delegations in 2017 – to the UK and Singapore. SINET61 will be run again in 2017, in partnership with the Growth Network, cementing Australia as a hub for bringing together cyber innovators, buyers and investors. And GOVPitch will bring innovative start-ups and scale ups to the Government's Digital Marketplace and connect solutions with buyers – government can set an example, supporting Australian industry by onboarding homegrown, high impact solutions.

The Australian Cyber Security Growth Network will increasingly engage with the Department of Industry, Innovation and Science, the Joint Cyber Security Centres and the Academic Centres of Cyber Security Excellence as they are established. Bridging the links between business, government and academia will create a fusion of Australia's cyber security expertise and identify new opportunities for investment, information sharing and research.

> *"Our commitment and ability to upgrade security infrastructure to meet increasingly sophisticated attacks is a major challenge of significant concern. This is an area where public-private partnerships to boost development of advanced sovereign cybersecurity solutions could be particularly effective."*
> ***Dr Jane Melia, Vice President of Strategic Business Development, QuintessenceLabs***

# A Cyber Smart Nation

## GOAL

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

The foundations of a cyber smart nation have been established, and outcomes are starting to show. We're building capacity in the tertiary sector with primary and secondary to follow. The conversation about diversity has been initiated, and now it's time for action. More work is required to increase the cyber security awareness message – government and business must unite and amplify.

> *"We have the talent, the capability, the universities. We have amazing work going on in the country to create a globally competitive cyber security industry."*
> ***Adrian Turner, Chief Executive Officer, Data61***

## DELIVERING THE STRATEGY

- Government has partnered with industry and academia to build research and workforce capability in cyber security by establishing Academic Centres of Cyber Security Excellence, with the successful institutions to be announced in 2017.
- Government is promoting pathways into cyber security careers by increasing the focus on science, technology, engineering and maths in our schools and universities.
- Starting the work to understand and address the causes of low participation by women in cyber security - currently around 11% globally - Government hosted a Women in Cyber event in March 2017 to engage women, industry and industry associations. The Office of the Cyber Security Special Adviser also launched a 'women in cyber' mentoring initiative in 2016.
- The flagship Stay Smart Online Week 2016 and other key events, including Safer Internet Day and World Backup Day, provided direct and digestible advice and raised cyber security awareness across Australia. Through Stay Smart Online Week in October 2016, it is conservatively estimated that government reached over 400,000 individuals and organisations - and many more through more than 1400 partners spreading the message through their own channels. Stay Smart Online Week also saw the Minister Assisting the Prime Minister for Cyber Security release an updated guide for small business and a new guide for individuals on how to be cyber secure.
- The Cyber Security Challenge has attracted a record number of participants and will be held in May 2017.

## BUILDING ON THE STRATEGY

Partnerships are springing up between government, industry, universities and TAFEs resulting in new vocational programs and cyber security degrees, doubling and trebling enrollments into existing cyber security degrees. Universities and TAFEs are adapting their curriculums in response to the Cyber Security Challenge and the job-ready employment needs of the Challenge's industry partners, Telstra, CISCO, Microsoft, Facebook, Commonwealth Bank, PWC, Splunk, BAE Systems and HackLabs.

Data61 and the Australian Institute of Company Directors have collaborated to lift the digital and cyber literacy of directors and boards across Australia. This initiative aims to create stronger and more secure organisations by facilitating a better understanding of cyber security by boards, appropriate risk management, the required investment and the opportunities for innovation that come with it. This collaboration aims to enhance the creation of highly-skilled company directors equipped to influence economic growth and community prosperity, while protecting enterprise assets from intentional theft or accidental loss. The collaboration is already achieving great success – Data61's cyber security webinar was the most watched in the Australian Institute of Company Directors' history.

The highly successful Australian Cyber Security Centre Conference – hosted by the Australian Cyber Security Centre in Canberra in March 2017 – continues to go from strength to strength, with increased speakers, participants and sponsors.

In the past twelve months, a number of industry associations, such as the Australian Information Security Association and the Australian Computer Society, have examined the cyber security skills problems and developed industry strategies to complement government initiatives. For example the Australian Computer Society is developing a certification framework for cyber security professionals.

The Stay Smart Online Alert Service continues to provide practical information to over 40,000 subscribers as well as providing general and targeted advice via its Facebook page with over 18,000 followers. Partnerships with industry build content and amplify messages through newsletters and websites. Government and industry are also driving cyber security messaging through the Security, Influence and Trust Group which brings together security awareness professionals from the Australasian region and includes representatives from major banks, retailers and telecommunications providers.

### QUESTACON

The National Science and Technology centre has been applying its unique approach to engaging audience in computer science, encryption and the development of 21st century skills in young people. Questacon's initiatives include Nkrypt, a science sculpture containing eight encrypted messages. Some have already been solved by a world-wide team of crackers while others remain a secret, development of teacher and student resources that introduce the ideas of codes, ciphers and cryptography, and the Bytewise travelling exhibition featuring 21 exhibits covering computer science, computational thinking, problem solving and cryptography. These will be critical capabilities in our future cyber security workforce.

## NEXT STEPS

While the higher education sector is an important and continuing focus, it is now time to connect and build on initiatives in our schools and TAFEs, including those initiated by industry and academia, such as the Victorian 'Cyber Games Initiative' and the girls coding network. Initial research will map the existing landscape of activity, to identify gaps, and opportunities for strengthening the student pipeline and skill base to support a world leading Australian cyber security work force. Opportunities will also be sought to collaborate on skills initiatives with international partners, such as New Zealand.

Arising from the Government's eCensus Review, a "Cyber Boot Camp" will be developed for Ministers and senior public sector managers, and a Cyber Lexicon will be created to build clarity around cyber security concepts. The Government, through the Office of the Cyber Security Special Adviser is also developing a 'Cyber Alumni' concept, to maximise the skills and networks of Australia's professional cyber security community.

The Government will align and, where appropriate, consolidate cyber security outreach programs across agencies. Research will ensure that education and awareness material is targeted to the most at-risk audiences and effectively influences the way people perceive, and act on, online risks. And a new Stay Smart Online website will be launched soon to improve the quality and discoverability of information for Australians.

The Cyber Security Challenge will run in May 2017 and includes assessment of more than just technical skills. Next year, the application process and competition will be redesigned to incorporate broader business skills to encourage technical and business collaboration.

> *"It's time to rise to the challenge and opportunity that cyber security presents. We can do this – as a nation."*
>
> *Dr Alan Finkel AO, Australia's Chief Scientist*

# Our Progress – Year One

○ Not scheduled to have commenced ● Progress ◐ Strong Progress ◉ Completed

| # | Action | Our Assessment | Lead Agency |
|---|---|---|---|
| A NATIONAL CYBER PARTNERSHIP | | | |
| 1 | Deliver progress updates on the implementation of this Strategy | ◉ | Department of the Prime Minister and Cabinet |
| 2 | Hold annual cyber security leaders' meetings | ◉ | Department of the Prime Minister and Cabinet |
| 3 | Streamline the Government's cyber security governance and structures | ● | Department of the Prime Minister and Cabinet |
| 4 | Sponsor research to better under-stand the cost of malicious cyber activity to the Australian economy | ○ | Department of the Prime Minister and Cabinet |
| STRONG CYBER DEFENCES – DETECT, DETER AND RESPOND | | | |
| 5 | 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 | | Australian Cyber Security Centre |
| | • co-designed joint cyber threat sharing centres (initially as a pilot) in key capital cities; and | | Attorney-General's Department |
| | • a co-designed online information sharing portal | | Attorney-General's Department |
| 6 | Increase the Computer Emergency Response Team (CERT) Australia's capacity | ◐ | Attorney-General's Department |
| 7 | Boost the Government's capacity to fight cybercrime in the Australian Crime Commission | ● | Australian Criminal Intelligence Commission |
| 8 | Boost the Government's capacity to fight cybercrime in the Australian Federal Police | ● | Australian Federal Police |
| 9 | Collaborate with Australian governments to ensure law enforcement officers receive the training they need to fight cybercrime across the nation | ● | Australian Federal Police and Attorney-General's Department |
| 10 | Increase the Australian Signals Directorate's capacity to identify new and emerging cyber threats to our security and improve intrusion analysis capabilities | ● | Department of Defence |
| 11 | Strengthen Defence's cyber security capacity and capability, through initiatives in the 2016 Defence White Paper | ◐ | Department of Defence |
| 12 | Expand the nation's cyber incident management arrangements and exercising program | ◐ | Department of the Prime Minister and Cabinet and Attorney-General's Department |

○ Not scheduled to have commenced ● Progress ◐ Strong Progress ◉ Completed

| # | Action | Our Assessment | Lead Agency |
|---|---|---|---|
| STRONG CYBER DEFENCES – RAISE THE BAR | | | |
| 13 | Co-design voluntary guidelines on good cyber security practice | ● | Attorney-General's Department |
| 14 | Continue to regularly update the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions | ◉ | Department of Defence |
| 15 | Co-design voluntary cyber security 'health checks' for ASX100 listed businesses | ◉ | Department of the Prime Minister and Cabinet |
| 16 | Support the Council of Registered Ethical Security Testers (CREST) Australia New Zealand to expand its range of cyber security services | ● | Department of Industry, Innovation and Science |
| 17 | Support small businesses to have their cyber security tested by CREST Australia New Zealand accredited providers | ● | Department of Industry, Innovation and Science |
| 18 | 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 | ● | Department of Defence |
| 19 | 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 | ● | Department of Defence |
| 20 | 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 | ● | Department of Defence |
| 21 | Develop guidance for Government agencies to consistently manage supply chain security risks for ICT equipment and services | ○ | Department of the Prime Minister and Cabinet |

○ Not scheduled to have commenced ● Progress ◐ Strong Progress ◉ Completed

| # | Action | Our Assessment | Lead Agency |
|---|---|---|---|
| GLOBAL RESPONSIBILITY AND INFLUENCE | | | |
| 22 | Appoint a Cyber Ambassador | ◉ | Department of Foreign Affairs and Trade |
| 23 | Publish an international engagement strategy on cyber security | ◐ | Department of Foreign Affairs and Trade |
| 24 | Champion an open, free and secure Internet to enable all countries to generate growth and opportunity online | ◐ | Department of Foreign Affairs and Trade |
| 25 | Partner internationally to shut down safe havens and prevent malicious cyber activity, with a particular focus on the Indo-Pacific region | ● | Department of Foreign Affairs and Trade |
| 26 | Build cyber capacity in the Indo-Pacific region and globally, including through public-private partnerships | ● | Department of Foreign Affairs and Trade |
| GROWTH AND INNOVATION | | | |
| 27 | Establish a Cyber Security Growth Network 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 | ◉ | Department of Industry, Innovation and Science |
| 28 | 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 | ◐ | Department of Industry, Innovation and Science |
| 29 | Work with business and the research community to better target cyber security research to Australia's cyber security challenges | ● | Department of the Prime Minister and Cabinet |
| 30 | Promote Australian cyber security products and services for development and export | ◐ | Department of the Prime Minister and Cabinet |

○ Not scheduled to have commenced ● Progress ◐ Strong Progress ◉ Completed

| # | Action | Our Assessment | Lead Agency |
|---|---|---|---|
| A CYBER SMART NATION | | | |
| 31 | Partner with Australian governments, businesses, education providers and the research community in a national effort to develop cyber security skills: | ◐ | |
| | • establish academic centres of cyber security excellence in universities; | | Department of Education and Training |
| | • 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; | | Department of the Prime Minister and Cabinet |
| | • continue to raise awareness in schools of the core skills needed for a career in cyber security; | | Department of the Prime Minister and Cabinet |
| | • understand and address the causes of low participation by women in cyber security careers; and | | Department of the Prime Minister and Cabinet |
| | • expand the Government's annual Cyber Security Challenge Australia to a broader program of competitions and skills development | | Department of the Prime Minister and Cabinet |
| 32 | Bring together and grow public and private sector cyber security awareness programs to make the best use of combined resources | ◐ | Attorney-General's Department |
| 33 | Work with other countries on cyber security awareness raising programs to deliver mutually beneficial outcomes | ◐ | Attorney-General's Department |

Australian Government