AUSTRALIA'S CYBER SECURITY STRATEGY:

EXECUTION & EVOLUTION

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

ABOUT THE AUTHORS

Zoe Hawkins
Zoe is an Analyst in ASPI's International Cyber Policy Centre, researching and writing on international and domestic cyber policy issues.

Liam Nevill
Liam is the Principal Analyst in ASPI's International Cyber Policy Centre, researching and writing on international and domestic cyber policy issues.

WHAT IS ASPI?

The Australian Strategic Policy Institute (ASPI) was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI INTERNATIONAL CYBER POLICY CENTRE

The ASPI International Cyber Policy Centre (ICPC) brings together the various Australian Government departments with responsibilities for cyber issues, along with a range of private-sector partners and creative thinkers to assist Australia in creating constructive cyber policies both at home and abroad. The centre aims to facilitate conversations between government, the private sector and academia across the Asia–Pacific region to increase constructive dialogue on cyber issues and do its part to create a common understanding of the issues and possible solutions in cyberspace.

The ICPC has four key aims:

- Lift the level of Australian and Asia–Pacific public understanding and debate on cybersecurity.
- Provide a focus for developing innovative and high-quality public policy on cyber issues.
- Provide a means to hold Track 1.5 and Track 2 dialogue on cyber issues in the Asia–Pacific region.
- Link different levels of government, business and the public in a sustained dialogue on cybersecurity.

We thank all of those who contribute to the ICPC with their time, intellect and passion for the subject matter. The work of the ICPC would be impossible without the financial support of our various funders, but special mention should go to the Commonwealth Bank, which has been a strong advocate and supporter of our work.

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

CommonwealthBank

THALES

.auDA .au DOMAIN ADMINISTRATION LTD

AUSTRALIA'S CYBER SECURITY STRATEGY:

EXECUTION & EVOLUTION

ZOE HAWKINS AND
LIAM NEVILL

CONTENTS

Executive summary 03

Introduction 04

Section 1: Strategy themes 05

1. Strong cyber defences 05
2. Global responsibility and influence 07
3. Growth and innovation 08
4. A cyber smart nation 08
5. A national cyber partnership 09

Section 2: Implementation challenges and improvements 13

Speed of delivery 13
Measuring success and understanding baselines 14
Communications 14
Human resources 14
Financial resources 15

Section 3: Moving forward—key recommendations 16

Strategy implementation 16
Private-sector engagement 16
The Australian public 17
Cyber governance 17

Appendix 1: Progress in achieving strategy outcomes 18

Key 18
National cyber partnership 19
Strong cyber defences 21
Global responsibility and influence 29
Growth and innovation 31
A cyber smart nation 33

Appendix 2: How much is the Australian Government spending on cyber issues? 35

Acronyms and abbreviations 40

EXECUTIVE SUMMARY

On 21 April 2016, Prime Minister Malcolm Turnbull launched Australia's Cyber Security Strategy, which outlined how the Australian Government will pursue the goal of 'enabling innovation, growth and prosperity for all Australians through strong cyber security'.[1] This report examines the strategy implementation journey of the past 12 months, through its successes and failures, and puts forward recommendations for government to help ensure that Australia's government, businesses and citizens can reach their cyber potential and thrive in the digital age.

The past 12 months has seen significant encouraging progress towards the goals of the strategy, thanks to commitment from both the government and the private sector. Efforts towards public and private sector collaboration have most notably manifested in the co-design of the ASX 100 cyber health checks and the launch of the pilot Joint Cyber Security Centre. This cross-sectoral cooperation hasn't been limited to addressing cyber threats but has also focused on developing Australia's digital economy. Government has been boosting the maturation of the domestic cyber start-up community through the Australia Cyber Security Growth Network and international Austrade 'landing pads'. Initiatives to attract, educate and diversify the country's cyber workforce to ensure the sustainability of Australia's cyber industry have also commenced.

The strategy called for the appointment of a new cyber leadership: a ministerial position and three key public service positions that lead cyber policy development on domestic, international and operational issues. This new cyber governance structure was put in place to drive the delivery of initiatives that contribute towards the strategy's five themes: strong cyber defences; global responsibility and influence; growth and innovation; a cyber smart nation; and a national cyber partnership.

Cyber issues have been afforded increasingly high levels of profile and transparency in the past year. Cyber Security Special Adviser to the Prime Minister Alastair MacGibbon's active engagement with media has helped make cybersecurity a front-page issue, while the Minister Assisting the Prime Minister for Cyber Security, the Hon. Dan Tehan MP, has made elevating the visibility of the public–private partnership his priority. Despite a delayed appointment, the new Ambassador for Cyber Affairs has hit the ground running and looks set to drive Australia's regional leadership and international engagement on cyber issues to new heights. At the same time, the government's greater transparency on Australia's cyber threats, incidents and capabilities has been a positive development for the country's cyber maturity.

However, the strategy's implementation has certainly faced its fair share of challenges and setbacks as well. Progress towards a national cyber partnership has been undermined by the ad hoc nature of government's communications and insufficient expectation management with industry partners. While some companies could show more initiative, the government also needs to more clearly delineate the division of responsibility within the national cyber partnership.

The very design of the strategy has been an obstacle to its implementation. Some of the document's outcomes are not quantifiable, so confidently measuring success is impossible. Many of the outcomes that are practically measurable are framed in terms of a relative change but are put forward without supporting baseline information necessary to measure progress. Disappointingly, the government's failure to enact a communications strategy associated with strategy's implementation has meant that a coherent and comprehensive narrative on implementation success has yet to be developed. This is not surprising, given that the human and financial resources afforded to the Department of the Prime Minister and Cabinet are simply not commensurate with the size and importance of the task.

Ultimately, some developments this year have been humbling litmus tests for the additional work that needs to be done to improve Australia's cyber posture. The results from a March 2017 ANAO audit of government departments revealed that a sub-par standard of cybersecurity was still in play in key agencies, raising questions about the take-up of the strategy's principles on the ground in government. The infamous 2016 #censusfail also revealed the pain points of Australia's cyber incident response capability, with inconsistent messaging coming straight to the fore.

That said, the confluence of leadership focus, the media spotlight and a mutual desire for public–private partnership means that the scene is set for Australia to learn from these implementation lessons and collectively move forward, committed to building on the successes of the past year.

1 Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy*, 21 April 2016, p. 5, online.

INTRODUCTION

The release of the Australian Government's Cyber Security Strategy on 21 April 2016 was welcomed by many as an important and necessary step in the evolution of cybersecurity in Australia. The new strategy broke a seven-year government silence on cyber policy issues since the launch of the 2009 Cyber Security Strategy penned by the Attorney-General's Department.[2] Since 2009, Australian governments have continued to tinker with the country's cybersecurity arrangements but haven't had a detailed and comprehensive plan on how to address the security and economic policy issues presented by the digital age.

Kevin Rudd's 2009 Defence White Paper emphasised the 'emerging threat' of 'cyber warfare' and established the Cyber Security Operations Centre in what was then the Defence Signals Directorate.[3] However, Rudd's anticipated Cyber White Paper failed to emerge after Julia Gillard took the prime ministership in 2010—a transition that pushed back a review of the government's cyber strategy until the current iteration. Gillard's tenure did see the transfer of cyber policy authority from the Attorney-General's Department to the Department of the Prime Minister and Cabinet (PM&C) in 2011, although it was hidden in the notes of a broader speech about a cabinet reshuffle, and her 2013 National Security Strategy created the multiagency Australian Cyber Security Centre (ACSC).[4] Meanwhile, other countries took leaps in best practice: the US launched two separate cyber strategies and the UK released cyber strategy documentation every year during that period.

The comparative absence of comprehensive cyber policy direction in Australia meant that the 2016 strategy had a significant void to fill. It needed to provide clarity on national cyber governance, boost confidence in cyber defences and stimulate cyber industry. Engaging the Australian private sector and public in a conversation about cyber policy and security was vital for national prosperity. Following a review of Australia's cyber governance and policy issues, the strategy's development was conducted by PM&C, advised by a panel of cybersecurity and business experts from Australia, the US and the UK. The projected release of the strategy in 2015 was significantly delayed by the ascension of Malcolm Turnbull to the prime ministership. However, the personal priority placed on the issue by Turnbull arguably elevated the public profile and political significance of the strategy when it was eventually launched in April 2016. Since that time, there's been significant activity both in and outside government on delivering the programs initiated by the strategy.

This report provides an accessible and critical appraisal of the government's implementation of the strategy over the past 12 months. Section 1 addresses each of the strategy's five themes, highlighting achievements and areas of weakness. Section 2 evaluates issues of execution, and Section 3 suggests ways to evolve the delivery and initiatives of the strategy to achieve its objectives. In addition to analyses of major themes, the report includes a table showing a detailed breakdown of progress against each initiative in the strategy's Action Plan, and another that examines the funding provided to achieve the objectives of the strategy.

2 Attorney-General's Department, *Cyber Security Strategy*, 2009, online.

3 Department of Defence, *Defending Australia in the Asia–Pacific century: Force 2030*, 2009, online.

4 'Australian cyber security centre to be established', media release, Department of Defence, 24 January 2013, online; 'Changes to the ministry', media release, Department of the Prime Minister & Cabinet, 12 December 2011, online.

SECTION 1: STRATEGY THEMES

The Cyber Security Strategy is divided into five major themes: strong cyber defences; global responsibility and influence; growth and innovation; a cyber smart nation; and a national cyber partnership. The themes are interdependent, but divide the strategy into more manageable and structured lines of effort towards achieving the strategy's overall goal of 'enabling innovation, growth and prosperity for all Australians through strong cyber security'.[5]

This conceptual framework is accompanied by an Action Plan outlining the individual steps that will be taken to realise the government's strategic goals. The ambitious list includes 33 initiatives, some of which were originally announced in the National Innovation and Science Agenda (NISA) in December 2015, and was allocated a funding package of $230 million for the next four years.

The following is a perception audit of the implementation of the strategy since April 2016. The analysis is based only on publicly available information and stakeholder perspectives on strategy delivery achievements and obstacles. We acknowledge that additional steps may have been made by government behind the scenes, but those activities fall outside the scope of this report, which is focused on increasing transparency about cyber policy developments from the perspective of the Australian general public, the private sector and academia. This discussion is also not intended to be exhaustive, but a more detailed breakdown of government progress against each action is in Appendix 1.

1. STRONG CYBER DEFENCES

Achieving a greater level of cybersecurity for Australia is one of the key overarching goals of the strategy and is necessary to ensure our national security and economic prosperity now and into the future. This task is multifaceted, and coordinated action is needed to improve both the security of government networks and the security of Australian businesses and individuals.

The Defence Department, specifically the Australian Signals Directorate (ASD), retains its leading role in safeguarding the Australian Government both through direct operational involvement in cybersecurity and through setting government cybersecurity standards. While some of ASD's work is necessarily secret, other areas are not, and the update of the its strategies to mitigate targeted cyber intrusions from the 'Top 4' to the 'Essential 8' is a clear example of the agency's critical role in Australia's national adaptation to evolving cyber threats.[6]

The *2016 Defence White Paper's* provision of $300–400 million funding for cybersecurity over 10 years will significantly assist Defence in this task. Not only will this facilitate the development of new technologies to monitor and defend Australia's networks, but the resources will help support the growth of its cyber workforce, which is essential to deliver this task. Similarly, efforts are underway to increase the capacity of CERT Australia and the Australian Criminal Intelligence Commission—a positive step for the country's cyber defences.

There have been increases not only in cyber defence capability but also in the maturity of Australia's transparency on its cyber posture and defences. The launch of the strategy was paired with Prime Minster Turnbull's announcement that Australia has an offensive cyber capability within ASD, and led to further discussion of the use of that capability against Islamic State in November 2016.[7] In addition, the release of the second annual ACSC *Threat report* provided increased transparency on the threats Australia faces and manages and the restrictions on the use of offensive capability. These developments have had a positive effect on Australia's efforts to build confidence and reduce the risk of conflict through greater transparency in the region.

Another key aspect of this theme is the *delivery of joint cyber security centres* in capital cities. Government is making steps towards this goal: the first of the centres was launched in Brisbane in February 2017, and more are expected to follow

5 PM&C, *Australia's Cyber Security Strategy*, 21 April 2016, p5, online.

6 *Strategies to mitigate cyber security incidents*, Australian Signals Directorate, February 2017, online.

7 'Launch of Australia's Cyber Security Strategy', Prime Minister of Australia, April 21 2016, online; 'Australia launches cyber war against Islamic State', *Australian Financial Review*, 22 November 2016, online.

later this year. Industry has welcomed the project and invested in its delivery, but there's been some frustration about the speed of delivery. Bureaucratic slowness, lengthy discussions and a focus on CEO-level approvals risks disengagement by private-sector partners who have invested time and human resources. This seems to be a symptom of the government's desire to have the pilot centre emerge fully formed, when an iterative approach that is faster would be more appropriate.

The co-design of *cyber health checks* for ASX 100 companies is another positive achievement in the first 12 months of the strategy. Further efforts to roll the checks out to mid-tier companies should be considered as a next step towards stronger cyber defence of Australia's private sector. The expected work to deliver the co-designed cybersecurity good practice guidelines will build upon this effort when it is completed. This is a complex problem, as many of these companies face some severe cyber challenges but don't have the internal capacity and resources to address them. This gap is more significant after increased regulatory requirements under new mandatory data breach notification legislation. Stakeholder feedback also indicates that future iterations of projects such as the ASX 100 health checks would benefit from using a split-survey design, in which questions on strategic management and risk issues go to company boards and chief executives, while operational questions are reserved for chief information security officers or their equivalents.

Another important step towards delivering stronger cyber defences is the new *Critical Infrastructure Centre* in the Attorney-General's Department. While not officially part of the Cyber Security Strategy, this initiative will help to achieve a stronger cybersecurity posture for Australia's critical infrastructure. There's currently only limited information publicly available on the centre, and greater transparency about its role for the cybersecurity of critical infrastructure would be welcome.

Unfortunately, a recent ANAO audit found that two key government departments have failed to fully implement the Top 4 mitigation strategies effectively and claimed that there was 'insufficient protection against cyber attacks from external sources'.[8] This finding and concerns over the 2015 Bureau of Meteorology hack mean that greater incentives and penalties must be established to ensure that government agencies meet their minimum cybersecurity standards. Doing so is essential for the government to lead by example by 'raising the bar' on this important issue.

Text Box 1: A new cyber governance structure

A key element of the government's effort to improve Australia's cyber posture was the establishment of 'clear roles and responsibilities'. The Cyber Security Strategy included the establishment of the role of the Minister Assisting the Prime Minister for Cyber Security, who supports the Prime Minister and engages directly with business leaders to deliver initiatives. This was paired with the creation of a new governance structure: a trio of cyber leadership positions spanning domestic policy, foreign affairs and operations. Clive Lines has continued to lead on Australia's cyber operations as the Coordinator of the Australian Cyber Security Centre, but the establishment of the new roles meant there was a need to find the right people for those jobs.

The first new role to be filled was that of the Special Adviser on Cyber Security, which was taken up by Alastair MacGibbon in May 2016. He has taken the lead on cyber policy development, spearheading coordination across departments in an effort to achieve a whole-of-government direction. Unfortunately, the relatively nascent public understanding of cyber issues in Australia has made it necessary for him to spend a significant portion of his time on front-facing public advocacy and media engagement, potentially at the cost of driving implementation at the coalface. In the face of this challenge, the Special Adviser has shown himself to be an energetic spokesman, demonstrating a pleasing level of transparency in his Census inquiry and agitating for change across the Australian Government.[9]

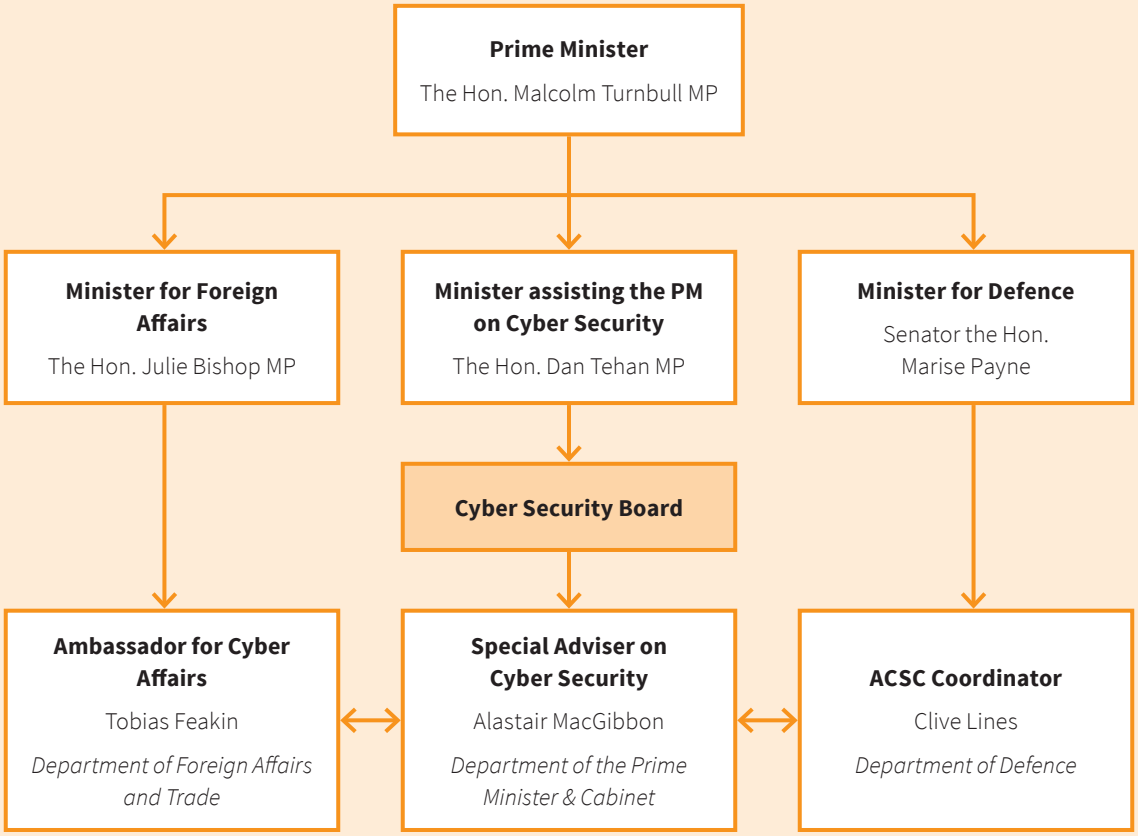
The Hon. Dan Tehan MP filled the Minister Assisting role in July 2016, and since that time has done a great job in regaining some of the momentum lost due to the length of the caretaker period in the months following the release of the strategy. He has successfully elevated public visibility of cyber issues through a full itinerary of speaking engagements and events. Unfortunately, the need to juggle the minister's commitments on cyber matters and his additional portfolios has limited the depth and detail to which he can delve into cyber policy. However, he has made a concerted effort to engage with industry on the topic, demonstrating government endorsement behind initiatives that industry has taken and advocating for broader participation in the effort. His quarterly meetings with business leaders are seen by industry to offer a good avenue for practical discussions on public–private partnership, and as a necessary complement to the high-level meetings with the Prime Minister.

8 *Cybersecurity follow-up audit*, Australian National Audit Office, 15 March 2017, online.

9 Alastair MacGibbon, *Review of the events surrounding the 2016 eCensus: Improving institutional cyber security culture and practices across the Australian government*, Office of the Cyber Security Special Adviser, 13 October 2016, online.

Dr Tobias Feakin stepped into the role of Australia's first Ambassador for Cyber Affairs in January 2017. His position within the Department of Foreign Affairs and Trade is a promising development for Australia's cyber leadership in the region; however, his appointment a full eight months after the launch of the strategy has left him with a lot of catch-up to do.

Broadly, this new governance structure has enabled the Australian Government to adopt a more coordinated approach to cyber issues across government. The establishment of key leadership positions has also gradually given a new voice to cyber issues, both for the Australian public and the region more broadly. It is under this governance umbrella that the goals of the strategy have been pursued, with varying degrees of success, over the past 12 months.



2. GLOBAL RESPONSIBILITY AND INFLUENCE

The Cyber Security Strategy astutely acknowledges the global nature of cyber issues and the associated importance of Australia undertaking a sophisticated international engagement strategy to promote and protect the nation's interests abroad. Unfortunately, the delayed appointment of the *Ambassador for Cyber Affairs* has hampered DFAT's ability to make many gains in cyber diplomacy since the launch of the strategy.

There's optimism that the appointment of Tobias Feakin as the Ambassador is a good step in the right direction on this front. Since taking up the role in January, Feakin has established DFAT's new *Cyber Cooperation Program*, a capacity building funding program that's part of Australia's official development assistance. The Ambassador is currently drafting a stand-alone *International Cyber Engagement Strategy*, with an open call for submissions, to ensure that Australia's efforts in this area are coordinated and effective.

Industry is already taking some action on international cyber issues, raising capacity around the region as a way of developing new and secure areas in which to conduct business. It's important that Australia's goal of a 'national cyber partnership' with the private sector is reflected in international efforts. The Australian private sector's knowledge and

overseas networks need to be leveraged to ensure that Australia's global cyber influence reaches its full potential. However, while the private sector is a force multiplier, in many cases government-endorsed efforts generate greater traction on the ground, so government must take a leading role to guide and coordinate Australia's cross-sectoral efforts in the international arena.

A key function of the forthcoming International Cyber Engagement Strategy will be to outline Australia's approach and priorities in regional cyber capacity building. In this sense, another sector with which the Ambassador should engage is the aid and development community, ensuring that lessons learned in that field are leveraged to inform the international strategy. A principle-based approach to capacity building should be adopted, including an effort to integrate cyber policy and development expertise, an increase in national and international coordination, and the creation of a sustainable and iterative approach to elevating cyber maturity in the region.[10]

3. GROWTH AND INNOVATION

The strategy's 'growth and innovation' theme acknowledges that cyberspace offers significant scope for economic growth and diversification. This is also addressed at a larger scale in the NISA, a $1 billion program announced in late 2015, which includes several initiatives that directly support the achievement of the strategy's goals.

The establishment of the *Australian Cyber Security Growth Network* (ACSGN) in December 2016 is a positive indication of action to better support the growth of Australian cyber companies. With support from Austrade, the ACSGN has supported engagement between Australian companies and the broader international cyber ecosystem, facilitating a delegation of 26 companies to visit the US for the RSA Conference and a separate delegation to attend Austrade's 2016 Australia–US Industry Week. The ACGSN also appears to be building strong links with CSIRO's Data61, which has a significant budget of over $70 million (see Table 6 in Appendix 2), to support cyber-related research and development. Austrade's *Cyber security industry capability report* is also a positive step towards increasing global interest in purchasing and investing in Australia's cybersecurity industry.

While the additional funding for cybersecurity research and support for cyber industries is welcome, stakeholder feedback has been critical of the apparently uncoordinated nature of some investment. Academic researchers, industry vendors and 'expert' consultants understand that there's never been a more lucrative time to talk about cyber issues, and greater oversight is needed to distinguish the most appropriate avenues for investment from opportunistic schemes. This process should ensure that there's a focus on achieving practical outcomes, not just a desire to demonstrate investment more generally.

The desire to increase the number of Australian cybersecurity businesses and exports and investment in Australian cyber services is admirable. However, the data necessary to assess the success or otherwise of this kind of goal is not yet available, and it's unclear whether anyone is collecting the information to enable that assessment. Steps towards baselining status quo industry statistics will be necessary to determine what success looks like on this front.

4. A CYBER SMART NATION

Without the people needed to fill cybersecurity jobs, and without a well-informed population, Australia faces a bleak cyber future. Initiatives under this theme seek to increase cyber skills and knowledge across the board and at all levels of sophistication. This theme can be broken into three pieces: building public awareness, developing a skilled workforce, and increasing the diversity of that workforce.

Public awareness

Pre-strategy public awareness campaigns have continued largely unaltered, but it's not clear that any work has been done to assess the efficacy of those campaigns and their continued utility. Public awareness campaigns such as Stay Smart Online need to be designed and expanded to create real behavioural change in order to make Australian society more cybersecure by habit.

This shouldn't involve just promoting the same facts all over again. In many cases, the issue isn't an absence of information about cyber risk but the lack of compelling engagement on what to do about it. The too common trade-off in technology between security and convenience leaves many people informed but unmotivated. Establishing innovative ways to operationalise public cybersecurity awareness into real behaviour change will require innovative approaches.

10 Mirko Hohmann, Alexander Pirang, Thorsten Benner, *Advancing cybersecurity capacity building: implementing a principle-based approach*, Global Public Policy Institute, March 2017, online.

Rather than mass awareness campaigns, government's limited resources may be better spent leveraging existing trust relationships in the community to inspire a shift in perspective. This should first involve bringing together cross-disciplinary experts such as psychologists and technologists to strategise about how to effectively market truly 'usable security' concepts. This should go beyond threat information and cyber hygiene tips and instead more persuasively make the case for a fundamental change in mindset in which proper cybersecurity practice isn't seen as a difficult and optional chore but as a new normal way of life. Tapping into established networks of community 'influencers' may be an effective method by which to propagate the concept; for example, there are lessons to be learned from the breast-cancer awareness efforts that have been run through hairdressers' salons.[11]

Growing the cyber workforce

Efforts to grow and diversify the cyber workforce will also be critical, and there have been positive developments towards that goal. The beginning of the process to establish academic centres of cyber excellence in February 2017 is a positive step; however, the funding available for this initiative is quite limited ($1.9 million over four years) and the inclusion of industry, for whom the graduates are being produced, appears to be haphazard at times.

In the past 12 months, there's been some growth in the number of tertiary courses focusing on cyber issues in Australia. The Australian Cyber Security Challenge continues to be a positive avenue through which to engage students on cybersecurity concepts, and efforts are underway to expand the scope of its activities. A potential expansion concept to aspire to could be a series of state/territory Cyber Security Challenges throughout the year, culminating in an annual Canberra-based national finale challenge.

At the same time, initiatives under the NISA are underway to boost digital literacy in primary and secondary schools and to incentivise further study in science, technology, engineering and mathematics (STEM) subjects. Naturally, it'll be several years before these students will graduate and be available to the workforce, and there's currently no clear baselining by which to judge any increase in the numbers or skills of graduates when they do. Undertaking and publishing research on cyber education and employment is an essential part of ensuring that this outcome is achieved effectively.

Cyber workforce diversity

The government has made noticeable efforts to increase the representation of women in the cyber industry in the past 12 months. Ensuring that women are aware of and have access to this career path is a vital ingredient in mitigating Australia's impending cyber workforce shortfall. The government has been proactively tackling the issue, building a 'women in cyber' component into the 2016 Australian Cyber Security Challenge, supporting female STEM students through NISA initiatives, and hosting events with women in the cyber industry to identify ways to improve female participation in the field.

Solving both the gender representation issue and the workforce shortage more generally essentially comes down to breaking two misconceptions. The first is that women can't or shouldn't take on technical roles; the second, which is arguably less discussed, is that the cyber industry needs only technical people. So, while increasing the number of women equipped to fill technical roles is a necessary ingredient for improving Australia's cyber workforce, it's certainly not sufficient. This isn't just a technology problem: in many ways it's a social problem, and Australia will flounder without diversity of skills in its cyber industry. The government needs to promote the fact that we also need informed legal minds, policy experts, communications specialists, psychologists and business risk managers. This should be done through broader engagement with universities outside of the STEM communities in order to tap into a wider range of skill sets. Government should consider incorporating a policy and governance element into the Australian Cyber Security Challenge in order to acknowledge the important role that such skills play in the cyber ecosystem and thus prompt young people from different backgrounds to consider a career in cyber policy.

5. A NATIONAL CYBER PARTNERSHIP

Achieving the outcomes under the first four themes of the strategy is underpinned by efforts to create a joint leadership model for cybersecurity between the public and private sectors. This reflects the multistakeholder nature of cyberspace, the scope of the challenges and the most efficient use of resources to address a shared problem. In this way, the strategy is a 'call to arms' for Australia. There's been significant activity in response, and both sectors have shown a genuine intention to collaborate. There's a strong sense of goodwill among the private sector and a willingness to collaborate with government from initiative endorsement to design and even funding, so now is a great time to capitalise on the partnership.

11 Health Western New South Wales, 'Bosom buddies booming across Western NSW', *Health Western NSW*, 14 September 2014, online; Lei Mei Li, 'A place for bosom buddies: salons spread awareness about cancer', *The Star*, 21 March 2014, online.

Unfortunately, issues of communication, expectation management and a lack of clarity on roles and responsibilities between sectors have somewhat undermined the benefits of that goodwill. Positive steps so far, and some of the issues noted above, are addressed in more detail below.

Senior engagement on cyber issues

As noted above, government leaders including Dan Tehan and Alastair MacGibbon have significantly improved the seniority, consistency and scope of engagement on cybersecurity with the private sector. In particular, Dan Tehan's initiative to establish quarterly industry meetings as a precursor to the annual meeting with the Prime Minister has been a welcome indication of the seriousness with which the government approaches engagement with the private sector. Similarly, Alastair MacGibbon has been an active and engaged advocate on cybersecurity issues, and his outgoing nature has helped to retain goodwill when there have been delays.

Threat information sharing

Government and the private sector have a mutual interest in sharing cyber threat intelligence effectively. The strategy lays out several initiatives to enhance this cross-sectoral flow of information, most notably through the establishment of a network of joint cyber security centres (JCSCs) and an online cyber threat sharing portal. This is a positive indication that the government is serious about improving the quality of information shared between itself and industry.

The official opening of the first JCSC in Brisbane in February 2017 is a good step in the right direction and demonstrates government follow-through on a strategy initiative. While industry advocated for a Sydney or Melbourne JCSC pilot, there are high hopes that a successful test centre in Brisbane will build the case for rollouts of JCSCs in the southern capitals. Media commentary indicates that the development of the threat sharing portal is underway but not yet complete.[12]

The November 2016 announcement of the relocation of the ACSC from the ASIO building to Brindabella Park was an encouraging acknowledgement that the national cyber partnership between government and industry couldn't achieve its full potential as long as the centre was contained within a high-security building. The swift execution of this move and the follow-through effort to deepen private-sector engagement will boost the success of the ACSC.

Some significant cultural hurdles on both sides must be overcome before the benefit of these developments can be truly realised. There's a perception among private-sector stakeholders that offering their information to the ACSC doesn't necessarily elicit a reciprocal information exchange from within government. This expectation of a one-directional transfer of data is undermining the business case for industry to get involved, and work needs to be done to build trust in reciprocity. In this sense, culture is still a bigger issue than geography or security limitations.

Communications and expectation management

The government has made a concerted effort to canvass private-sector perspectives on certain cyber issues and has used those insights to shape the delivery of various strategy initiatives. This is a positive development, as it shows an acknowledgement of industry experience and expertise on the topic.

However, true partnership is built on more than a one-time data collection exercise. It relies on frank, frequent and reciprocal communication. Stakeholder interviews have indicated that there's often a lack of follow-through from government interlocutors on strategy implementation issues. Information on timelines and priorities has been difficult to obtain, and consultation has been followed by long delays in action or communication. Many stakeholders expressed a keen desire for more frequent communications with government, even when there's no substantive action to report. There needs to be more outward data distribution from government in the form of updates and follow-ups to the private sector, notifying it of achievements, potential delays or priority shifts.

Ensuring that this type of sustained two-directional dialogue is achieved means moving away from ad hoc engagements and towards a structured system of communication with industry. Simple concepts such as a weekly newsletter available by subscription could offer a go-to source of information for interested private-sector partners. The NISA offers an email update service, and the newly established ACSGN has created the option to become a 'Friend of the Network'.

This is a useful mechanism by which to increase transparency. The government should consider establishing a similar mass update function dedicated to the implementation of strategy initiatives. This kind of regular, routine update could explain the reasons for an absence of action or delays or, if not, at least confirm that work on implementation is continuing to some extent, or when it's expected to commence. Furthermore, stronger communications from government to stakeholders may help to clarify lead agencies and individuals with responsibility for particular actions. Some stakeholders are unfamiliar with

12 'Government launches Joint Cyber Security Centre in Brisbane', *Computer World*, 24 February 2017, online.

government practices, and the clarification of expected timelines, responsibilities and processes may assuage many of the concerns expressed during our stakeholder consultation about progress on the strategy.

Delineation of responsibility

The importance of cyber policy issues and their ubiquity across the government, private and civil sectors highlight the necessity of the strategy's national cyber partnership approach. In practical terms, the concept of co-leadership means that the private sector should take on some responsibility for the implementation of the strategy. By extension, both the public and the private sectors should be held accountable to some extent for the success or failure of the strategy.

However, the exact division of responsibility between government and the private sector for advancing Australia's cyber maturity is difficult to define. While the intent for the private sector to be a partner of government has been expressed in the strategy and associated rhetoric, stakeholders have voiced frustrations that there's insufficient clarity on exactly where and how they should step in.

While both the public and the private sectors are eager for more involvement from the other, the strategy ultimately remains a government document. As such, it would be most effective if government, in consultation with stakeholders, were to ascribe leadership roles for certain initiatives to particular industries or organisations that have a specific interest in achieving the outcome. This sort of clear division of responsibility would enable companies to plan, invest and take action accordingly, ideally resulting in an alleviated implementation burden for government.

This approach will also require a higher degree of proactive engagement from the private sector across the board. Large companies have the opportunity to play a coordinating role for groups of companies that share an interest in specific initiatives in order to streamline industry collaboration with government. Clearer government guidance on useful areas for private-sector action will give companies a clear window to take ownership of an endeavour, allowing private-sector underparticipation to be more effectively identified.

Text Box 2: Measuring effectiveness

Measuring the effectiveness of the Strategy's 33 initiatives is critical to understanding if they are achieving the desired outcomes. This requires the collection of qualitative and quantitative data, prompting the Strategy's commitment to 'Sponsor research to better understand the cost of malicious cyber activity to the Australian economy'. However despite its criticality to assessing the effectiveness of Strategy initiatives, the first annual update notes that work on this has only reached the initial scoping stage of new research efforts. It also notes that this will be done in conjunction with the private sector. The private sector already has a significant body of highly relevant data that can be used to assess the growth of cybercrime issues such as phishing in Australia.

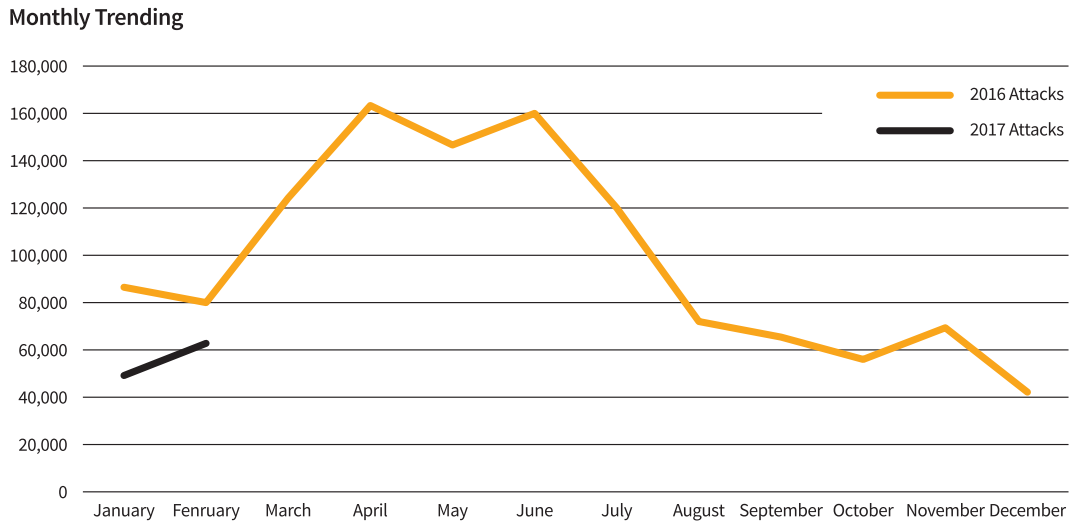
The information below, provided by online brand protection company MarkMonitor, shows the volume of phishing attacks on the 'Big Four' Australian banks detected by MarkMonitor in 2015 and 2016. The graph shows worldwide phishing attack trends in 2016 compared to 2017.

Government should look to leverage data collection capabilities that already exist in the private sector when pursuing their national research efforts.

TABLE 1: PHISHING ATTACKS AUSTRALIAN FINANCIAL INSTITUTIONS

Organizations	Industry	Estimated Detection Volume 2015	Estimated Detection Volume 2016
ANZ Banking	Financial	2,233	2474
Westpac Bank	Financial	1,411	4547
National Australia Bank	Financial	1,941	3006
Commonwealth Bank	Financial	761	930

FIGURE 1: PHISHING ATTACK TRENDS WORLDWIDE



* Attacks detected by MarkMonitor. Not intended as an industry-wide summary.

Information supplied by MarkMonitor. The data may not reflect all data available.

SECTION 2: IMPLEMENTATION CHALLENGES AND IMPROVEMENTS

This section discusses the overarching challenges identified in the above assessment of strategy implementation under its distinct themes. The following gap analysis informs discussion of recommended improvements to facilitate the implementation of the strategy in Section 3. Overall, we have found that the speed of delivery, poor communications and human resource limitations have affected implementation.

SPEED OF DELIVERY

The strategy's Action Plan shows that significant attention was paid during its development to how the objectives of the strategy would be realised. Unfortunately, the extended caretaker period associated with the 2016 federal election and the subsequent adjustments within the ministry and government meant that there was a noticeable lull during which little happened after the strategy's launch. While this delay was unavoidable, it meant that the strategy's implementation and the progress of Australian cyber policy were behind the strategy's (nonexistent) schedule before it even began.

Since that time, there's been significant effort to implement the Action Plan, which has delivered on several outcomes, as demonstrated in Appendix 1. However, the absence of an initiative delivery timeline has undermined clarity and led to different expectations of implementation speed in the public and private sectors, stoking concerns about the government's commitment to implementation. The lack of detailed information on this front means that there's no indication of how fast and in what order things will be done, other than from inferences that can be drawn from the observation that funding is allocated across the forward estimates to 2019–20 (see Appendix 2 for details).

A detailed delivery timeline would be a useful way to communicate to industry and civil society specifically which areas the government considers as priorities for immediate implementation and which ones it deems to be more long-term goals. Without this guidance, stakeholders have less information with which to prepare their contribution to, or participation in, particular initiatives. Communicating a timeline would lead to greater coordination of resources and facilitate a more efficient delivery of the strategy, with all parties working in concert to achieve shared goals with clear priorities.

Failure to provide a timeline has opened the government up to criticism, since stakeholders are left with nothing but their own expectation against which to judge the pace of activity. There's a perception among stakeholders that implementation is slow and that the speed of tangible on-the-ground delivery isn't yet commensurate with the importance of the issue or reflective of the government's narrative of urgency.

Minister Tehan recently offered his assurance that the government was 'making implementation of the strategy ahead of time a priority' in the light of the pace of change in cybersecurity developments.[13] However, this promise to deliver outcomes ahead of schedule remains vague when there's no clear original timeline against which to test it. The government needs to develop a clear road map with timelines, milestones and deliverables. Separate annual implementation plans for each strategy theme could be a helpful way to articulate the practical how, when and who of each initiative. Releasing annual iterations will ensure that the approach evolves with the environment and that stakeholders always have an up-to-date understanding of implementation expectations.

13 Annabel Hepworth, 'Dan Tehan ramps up cyber strategy to get ahead of threat to power', *The Australian*, 9 March 2017, online.

ANNUAL UPDATES AND MEASURING SUCCESS

The Strategy committed government to publish an annual update on progress of the Strategy, the first of which was published on 19th April 2017. The update provides summaries of actions taken so far, work planned for the next 12 months, and identifies a few areas in which it intends to make improvements. However it is almost devoid of critical self-assessment, and its approach to the review process is flawed.

The update outlines a plan to publish a 'view of the cyber security ecosystem' to overcome structural ambiguity within government and 'mature its communication channels' to address the paucity of regular public updates. It also flags the intention to release an update of the 2013 National Plan to Combat Cybercrime, and a greater focus on small business. There are plans to improve coordination between the federal and state and territory governments, and the private sector to make Australia's critical national infrastructure cyber secure, led by the new Critical Infrastructure Centre within the Attorney-General's Department, along with the ACSC.

Unfortunately, the update is artfully forgiving. For example, it refers to government cyber security audits by the Australian National Audit Office, but omits any reference to the audit's worrying revelations of poor cyber resilience in key government agencies. It also relies on hypothetical victories, referring to a study that predicts an uptick in cybersecurity investment. However the study quoted makes the prediction based on a 'shift in thinking around cyber security' and 'if Australia invests further in cyber security' rather than on the current trajectory.

The general lack of transparency around strategy delivery timelines that plagued the past 12 months has carried into the first annual assessment and its table of progress on the 33 initiatives. The absence of timelines leaves the government room to mask underperformance, and means that promises to 'accelerate' or deliver initiatives 'ahead of schedule' hold very little meaning. Upon closer inspection of the table of progress, it's obvious that its focus on actions, rather than outcomes is a critical methodological failing. Best practice policy evaluation recommends assessing the extent to which intended and unintended outcomes are achieved. Merely stating that an action was undertaken doesn't clarify whether the desired effect was achieved, or if the action is still the most appropriate way to achieve the end goal. In doing so, an opportunity has been missed to explain what has changed because of Strategy implementation efforts.

Assessing the implementation of this strategy is impeded by the lack of clarity on exactly what success looks like, and how it could feasibly be measured for each outcome. For example, 'all businesses benefit from cyber security solutions commercialised with Growth Centre support' is so abstract as to be meaningless in terms of quantifiable progress produced by the time and money invested in the strategy.

Other outcomes in the strategy discuss variables that are quantifiable but rely on the measurement of a relative change—for example, 'the number of cybersecurity graduates increases'. This reasonable aspiration is undermined by the absence of any data against which to measure the change. The government needs to publish baseline research on these indicators so that any positive future trend, or 'success', is identifiable. Doing so would not only make it possible to conduct cost–benefit analyses of certain strategy initiatives, but also assist the achievement of other initiatives aiming to increase the quantity and quality of Australian cybersecurity research.

COMMUNICATIONS

Actions speak louder than words, but a good communications strategy is vital in order to translate practical efforts and investments that the government has made into awareness and understanding among the general public, the media and civil society.

Cyber issues have certainly been given greater profile thanks to the strategy. Minister Tehan's and Special Adviser Alastair MacGibbon's advocacy, particularly on discussions about the importance of skill development and critical national infrastructure protection, has raised the importance of the issue for the Australian people. However, a good communications strategy doesn't just mean volume, but establishing a narrative that's both targeted and coordinated. As Appendix 1 suggests, there's still a gap between the good work being done on strategy initiatives and the public perception of delivery. There's scope for a more robust communications strategy within PM&C to create a consistent and proactive narrative informing the public of both strategy wins and delays.

Government also needs to be equipped to swiftly establish a coordinated communications strategy in response to any cyber incident that may arise. The #censusfail scenario revealed a plurality of narratives on the nature, severity and significance of a cyber incident that caught the nation's attention. It was apparent that there wasn't a pre-planned overarching communications strategy. Delivering a more coherent narrative and a unified government position is essential to sustain public confidence in the government's approach to cyber issues. This is as important an asset for government as it is for the private sector. Establishing a more mature communications strategy development process that comes into play

in the wake of a cyber incident, including an accurate and truthful description of what happened, common language, media management and a key spokesperson, will help to ensure that the government can convey its situation assessment and incident response intentions in the most reassuring and coherent manner possible.

HUMAN RESOURCES

The implementation of the strategy is a task of nationally significant scope and scale, but in practice there are precious few people tasked with driving its achievement. The government's coordinating agency, PM&C, has a small team led by Alastair MacGibbon and focused on delivery. However, our budget assessment in Appendix 2 reveals that PM&C was not provided with any additional funding with which to implement the strategy. While we have made much of the positive effect of MacGibbon's strong public profile, it may be that this has come at the expense of the time and effort needed to drive the internal leadership of the implementation. Leading the public commentary, developing policy and implementing the strategy are a nearly impossible task for the team with its existing size and scope. Expanding the team within PM&C to include more individuals, some with purely public-facing roles and others with internally focused coordination responsibilities, may alleviate pressure and facilitate the achievement of the cybersecurity objectives.

Similarly, Minister Tehan has been an energetic advocate of cybersecurity issues, but his extensive portfolio, which also includes being Minister for Defence Personnel, Minister for Veterans' Affairs and Minister Assisting the Prime Minister for the Centenary of Anzac, means that cybersecurity can't be his primary focus. Achieving the significant work detailed in the strategy may demand the appointment of a minister focused solely on cybersecurity, or with somewhat less demanding additional portfolios than Mr Tehan currently manages.

FINANCIAL RESOURCES

When the strategy was released, the government announced associated funding of 'about' $230 million, including $38 million of previously announced initiatives from the NISA. The analysis in Appendix 2 shows that this funding was certainly provided in the 2016–17 Budget, albeit largely through the redirection of existing Defence funding to other agencies and initiatives.

As noted above, achieving the strategy's outcomes will require significant leadership and coordination from PM&C. It's noteworthy, in the context of concerns about communications, the speed of delivery and the overloading of personnel in key leadership roles, that PM&C wasn't provided with additional appropriation to manage the delivery of the strategy. Similarly, the Department of Foreign Affairs and Trade (DFAT) will also fund the $6.7 million announced in the strategy through the redirection of existing appropriation.

The pace of delivery of the strategy and stakeholder communications may be improved if funding for additional human resources can be provided to drive implementation at a quicker pace. If support can't be increased, then it may be necessary to rationalise the initiatives, prioritise them based on need, and leverage the private sector more effectively.

There's been some criticism of the amount of funding allocated for the delivery of the strategy. When the funding has been compared to the size of the task, questions have been raised as to whether it's enough to support the strategy's ambitions.[14] While it's important to make cyber budget comparisons to the US and the UK on a proportional rather than gross basis, Australia does spend less on cybersecurity that its allies.[15] The long absence of strategic direction makes it somewhat understandable that funding may be tracking behind that of other countries that have been more consistent in their development of related policy. However, there are concerns that this is currently manifesting in a government willing but unable to deliver on the ambitious goals set out in the strategy.

This context makes the recommendation to better leverage private investment even more important to achieving the outcomes of the strategy. As noted elsewhere, this will require a more definitive division of responsibilities between the public and private sectors.

14 Greg Austin, Jill Slay, *Australia's response to advanced technology threats: an agenda for the next government*, May 2016, online.

15 Zoe Hawkins, Liam Nevill, 'National cyber budgets: same same but different', *The Strategist*, 16 June 2016, online.

SECTION 3: MOVING FORWARD—KEY RECOMMENDATIONS

The government is clearly committed to trying to deliver what it promised, but challenges remain that may undermine the success of action to achieve the strategy's outcomes. In this section, we discuss a series of short-, medium- and long-term recommendations to improve the execution, adaptability and delivery of nationally important cybersecurity outcomes.

STRATEGY IMPLEMENTATION

Recommendation 1: Rapid adaptation and evolution

Alastair MacGibbon has previously advised that relying solely on a 'tick box' compliance culture is a limited approach to such a complex issue.[16] The first annual update was an opportunity to take a more flexible and adaptive approach to the implementation of the Strategy. This should have been based on an assessment of the extent to which intended outcomes have been achieved so far, and changing focus where necessary. However the first annual update only seems to have assessed actions, not outcomes, and in doing so an opportunity has been missed to explain what has changed because of Strategy implementation efforts.

It's important to follow through on government strategies, but it's even more important to ensure that the measures that are being implemented are adapted to changes in the environment. Merely stating that an action was undertaken doesn't clarify whether the desired effect was achieved, or if the action is still the most appropriate way to achieve the end goal. Instead, government should adopt a spiral development approach to the strategy, using future annual updates as an opportunity to abandon initiatives that no longer make sense and adding new ones as new opportunities or challenges arise. There's a broad agreement with the stated objectives of the strategy, but a focus on execution and adaptation is necessary, evolving as our understanding of more effective and efficient methods and initiatives by which to achieve those objectives grows.

Recommendation 2: Measurable and time-bound annual action plans

Government should review the Action Plan annually, possibly in connection with its quarterly and annual industry meetings. Releasing new theme-specific action plans that provide clear timeframes and measurable milestones for activity will enable implementation and private-sector cooperation. It will also increase accountability among responsible government leaders and facilitate better expectation management for the private sector and general public.

Recommendation 3: Undertake baseline research

Understanding the effectiveness or otherwise of cybersecurity initiatives requires robust data to measure progress against. Funding should be provided to undertake and publish targeted strategy-specific research, which will improve the government's ability to measure strategy success while boosting Australia's cyber research portfolio.

PRIVATE-SECTOR ENGAGEMENT

Recommendation 4: More open communications with the private sector

Communicating progress, or reasons for delays, will significantly facilitate the development of a trusted and execution-driven national cybersecurity partnership. Measures such as quarterly threat reporting from the ACSC and regular strategy updates, potentially in the form of a newsletter, would give stakeholders confidence in the commitment to action and delivery.

16 Paris Cowan, 'Govt undermined by "tick box" security culture: MacGibbon', *itnews*, 23 March 2017, online.

Recommendation 5: Define the division of leadership between sectors

The strategy is a government-developed, government-owned document, but it is not solely the responsibility of government to deliver it under the partnership model. Working with industry to define which tasks government wants industry to deliver—and obtaining industry buy-in to do so—will further enable the delivery of outcomes and the growth of this partnership.

Recommendation 6: Better support for mid-tier and small to medium enterprises

There's likely to be an expectation that improved cybersecurity in the top end of town will trickle down to the mid-tier, but evolving threats and government regulation make it unrealistic to expect that this will happen in the timeframe needed. Greater government support to help small and medium enterprises comply with incoming data breach notification legislation is required before the legislation takes effect. The government could consider measures taken to assist business with other regulatory transitions, such as the implementation of the GST, as examples of measures to provide practical assistance.

THE AUSTRALIAN PUBLIC

Recommendation 7: Better communications with the public in both implementation and crises

Having a strong and coherent communications strategy for the Australian public is essential to the success of the strategy. This involves better coordination of front-facing discussions on the implementation of the strategy. It's also necessary to have the ability to quickly establish clear and accurate crisis communications should a cyber incident arise. This two-pronged effort should be supported by a greater communications capacity within PM&C.

Recommendation 8: Moving from public awareness to behavioural change

Growing the cybersecurity understanding of the general public to the extent that there are obvious behavioural changes is a key way to achieve greater national security and reduce rates of cybercrime. New methods of education and awareness raising that change behaviours positively should be developed and implemented. The government should look for lessons learned from other awareness-raising programs (for example, those focusing on breast cancer) that leverage existing trust relationships in the community to inspire a shift in mindset.

Recommendation 9: Broaden the conception of cyber skills shortages to include other necessary disciplines

There's a perception that cybersecurity is principally a technical issue and that therefore more technically skilled people are needed. While that's true, it misses another piece of the puzzle: a growing industry needs a variety of disciplines to support technological advances comprehensively. When examining skills shortages, government should look beyond the technical community. Individuals with backgrounds in law, psychology, government studies, communications and many other disciplines have an important role to play in ensuring that Australia's future cyber workforce is equipped to deal with the full spectrum of challenges that cyberspace presents. This should be reflected in broader engagement through education initiatives such as university careers fairs and Australia's Cyber Security Challenge.

CYBER GOVERNANCE

Recommendation 10: Provide additional financial and human resources to strategy delivery roles

The delivery of the Cyber Security Strategy demands a focus on execution and sufficient financial and human capital to manage implementation across many portfolios and private-sector partners. Consideration should be given to supplementing personnel in these roles and providing additional support to senior leadership positions or rationalising their other tasks to facilitate a focus on the achievement of better cybersecurity outcomes.

Recommendation 11: The co-location model of the ACSC should be examined for use by policy agencies

The evaluation of the strategy in this report reveals the dispersed leadership of many of the policy initiatives discussed. Elements of cyber policy responsibility are found in PM&C, the Department of Defence, DFAT, the Attorney-General's Department, and so on. This can be challenging for those responsible for coordinating the delivery of the initiatives. While an agency along the lines of Singapore's Cyber Security Agency may not be the most appropriate response for the Australian Government, the co-location of key personnel may help to streamline the delivery of policy initiatives and enhance engagement between policy agencies and the operational cyber areas of the government. It would also aid engagement with the private sector by providing a one-stop shop for engagement with the senior cyber officials in the Australian Government.

APPENDIX 1: PROGRESS IN ACHIEVING STRATEGY OUTCOMES

The table below provides comments against each of the 84 outcomes presented in the Action Plan attached to the Cyber Security Strategy, and an assessment of progress using colour coded ratings, the key for which is at the end of the table. When reviewing the outcomes, note that the Action Plan has been devised in the context of at least four years of expected delivery. Therefore, it's to be expected that many of the initiatives won't have started yet, as they rely on the outcome of other work, or departments may not yet have the capacity or budget to commence them; those outcomes are indicated by grey in the rating column. As mentioned in this report, some of the strategy outcomes are not objectively measurable; those outcomes have been highlighted by black in the rating column.

KEY

Rating	Description
	Outcome achieved.
	Significant progress towards achievement.
	Underway, but more work is required.
	Not started.
	Dependent on achievement of outcome.
	Outcome is either unquantifiable, lacks an indicator against which to measure progress, or the information is not publicly available.

NATIONAL CYBER PARTNERSHIP

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

Action	Outcome	Progress to date	Rating
1. Deliver progress updates on the implementation of this strategy	a. The Government evaluates its implementation progress and updates this Action Plan annually	The government released the *First Annual Update* on 19 April 2017.	
2. Hold annual cyber security leaders' meetings	a. The Prime Minister and business leaders set the strategic cybersecurity agenda and drive the Cyber Security Strategy's implementation from the top down	The meeting between the Prime Minister and business leaders took place on 19 April. Minister Tehan has also pledged quarterly meetings, two of which have been held so far in December 2016 and March 2017.	
	b. Business leaders and the Government are equipped with the information they need to make appropriate investment and business decisions on their cybersecurity, including a collective understanding of emerging cyber challenges	The government has acknowledged the importance of improving the information exchange between the private sector and government on the topic of cybersecurity through the Prime Minister's business leaders' meetings, the first of which was held in mid-April 2017. Annual meetings are insufficiently frequent to achieve this outcome, given the pace of change in the cyber threat environment, so it's pleasing to see the introduction of Minister Tehan's quarterly business roundtable to fill that gap. Those meetings have so far been held in December 2016 and March 2017. The cybersecurity business guides published by Stay Smart Online are also useful information on good cyber practices, but greater research needs to be undertaken for government and business leaders to make truly informed judgements about the cyber risk and investment dynamics in Australia.	

Action	Outcome	Progress to date	Rating
3. Streamline the Government's cyber security governance and structures	a. Government responsibility for cyber security is well communicated and understood by stakeholders	The appointment of Minister Tehan and Alastair MacGibbon has provided more clarity about cyber leadership in the Australian Government. There is also the Cyber Security Board, chaired by the Secretary of PM&C, but its functions and activities are opaque. Governance structures and the division of responsibility within government are not well articulated in accessible documentation, and more work can be done to demystify those structures for the public.	
	b. The Prime Minister appoints a Minister Assisting the Prime Minister on Cyber Security	Dan Tehan MP was appointed the Minister Assisting the Prime Minister for Cyber Security on 18 July 2016.	
	c. The Government's cyber security operations are coordinated, efficient and align with strategic priorities	This is difficult to assess from an external perspective, but revelations in the second annual ACSC *Threat report* and cybersecurity audits of government departments by the ANAO indicate that, while the operational response is strong, departments are often falling behind in their cybersecurity obligations. The bitter experience and lessons of #censusfail highlighted that there's still work to be done to refine the government's cyber incident response arrangements.	
	d. 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	In November 2016, the government announced plans to relocate the ACSC from the ASIO building to Brindabella Park at Canberra Airport by the end of 2017.	
4. Sponsor research to better understand the cost of malicious cyber activity to the Australian economy	a. A better understanding of the economic impact of cyber compromises to the Australian economy is developed	No information on progress towards this outcome was discovered.	
	b. Robust data is published that supports informed decision making on cyber security risk management and investment	No information on progress towards this outcome was discovered.	
	c. Robust data is published that improves the ability of organisations to consider the effectiveness of their investment in cyber security	The ACSC *Threat report* and the 2015 Cyber Security Survey provide some useful information for business to consider, but government has not yet provided robust data to achieve this outcome.	

STRONG CYBER DEFENCES

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

Action	Outcome	Progress to date	Rating
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; • co-designed joint cyber threat sharing centres (initially as a pilot) in key capital cities; and • a co-designed online information sharing portal	a. Partnerships between the Australian Cyber Security Centre and the private sector are increased and proven valuable for both parties	It is difficult to measure this outcome. There appears to be more engagement between industry and the ACSC—a trend that we hope will increase with the centre's relocation. However, whether it has proven valuable for both parties isn't objectively measurable.	
	b. An operating model for the joint cyber threat sharing centres is developed, successfully piloted and reviewed	In October 2016, it was announced that a pilot centre would open before the end of 2016. The first pilot joint cyber security centre (JCSC) eventually opened in Brisbane on 24 February 2017. There is clearly mutual intent from government and the private sector to ensure the success of the JCSC program, but progress so far has been slower than some stakeholders expected, and the pilot's location in Brisbane rather than Sydney or Melbourne has been questioned. As the centre isn't yet fully operational, more time will be needed for an effective review process to take place.	
	c. 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	This action relies on an assessment of the pilot JCSC opened in February 2017 in Brisbane. Additional time for the pilot centre to reach full operational capability will be needed before an assessment of the pilot and a subsequent rollout of the model to other cities in Australia.	
	d. Cyber security information is delivered to a wider range of organisations through the online information sharing portal	Media commentary suggests that CERT Australia, within the Attorney-General's Department, has begun work on developing the threat information sharing portal, although the absence of concrete announcements indicates that it's not yet operational.	

Action	Outcome	Progress to date	Rating
6. Increase the Computer Emergency Response Team (CERT) Australia's capacity	a. CERT Australia's services are expanded for a wider group of businesses, with improved technical capability	The announcement of a new CERT Australia recruitment campaign in August 2016 is a positive step towards increasing the organisation's capacity to deliver the five initiatives allocated to it in the strategy.	
	b. CERT Australia increases its international partnerships, focusing on prevention and shutting down malicious cyber activity	The onboarding of additional staff is intended to improve CERT Australia's capacity to increase its international partnerships and the fight against cybercrime. While the organisation's website has not yet posted any news items to this effect, undertaking the necessary boost in staffing will contribute to the realisation of this partnership expansion.	
7. Boost the Government's capacity to fight cybercrime in the Australian Crime Commission	a. The Australian Crime Commission increases its capacity and capability to detect and analyse cybercrime	Australian Criminal Intelligence Commission has received funding for further investment in cybercrime investigation capability, and the government advises that a successful employment drive has seen its intelligence unit double from 6 to 12 personnel.	
8. Boost the Government's capacity to fight cybercrime in the Australian Federal Police	a. The Australian Federal Police increases its capacity and capability to investigate cybercrime.	The AFP has received funding for further investment in cybercrime investigation capability; however, there is no data to measure the success of this investment so far.	
9. 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	While no information is available to suggest that this has commenced, the government advises that this work is underway.	
	A specialist training strategy is developed and implemented	While no information is available to suggest that this strategy has been developed or implemented, the government advises that internal cyber training activities are underway and that a specialist training strategy will be included in the forthcoming National Plan to Combat Cybercrime.	
10. 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	Through funding provided in the Defence White Paper, ASD has been very active hiring new staff for cybersecurity roles. However, the nature of this capability and ASD's activities makes it difficult to assess whether the agency's capability or capacity has increased.	
	The Australian Signals Directorate expands the number of cyber security services it offers to a wider range of organisations	Again, the achievement of this outcome is challenging to judge from open-source research. However, it's fair to assume that this expansion of service is reliant on the delivery of the above mentioned increase in ASD capacity and capability.	

Action	Outcome	Progress to date	Rating
11. 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 has been recruiting to increase its cyber workforce across defensive and offensive roles, indicating that there's action towards the achievement of this outcome.	
	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	Some details of this outcome are necessarily secret, so there's little solid public data on which to assess its achievement. However, given that Defence appears to be making steps towards improving its cyber capabilities (as noted above), it stands to reason that there will be an associated increase in the resilience of Defence networks.	
12. 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	Revised cyber incident management arrangements have been developed, and an exercise to test was held with the private sector in April 2017. Updating the arrangements was also a recommendation of the *Review of the events surrounding the 2016 eCensus*, published by the Office of the Cyber Security Special Adviser.	
	Australian governments understand how their respective cyber and incident response teams would operate together in a cyber crisis	Revised incident management arrangements have been developed, but achieving this outcome will require significant testing. Government advises that testing of the cyber incident management arrangements with private industry and the federal and state governments commenced in April 2017.	
	The Government and private sector establish a program of joint cyber exercises	Joint cyber exercises between government and industry have been under development. The first iteration took place in April 2017. Government advises that exercise development was originally intended to take place during 2016–17, and that the first exercise was not scheduled to be conducted until 2017–18.. Unfortunately, private-sector uncertainty over the progression of this project means more work is required.	
	Australia works with international partners on developing policies for incident response as a confidence building measure	Ministers from Australia and New Zealand committed in October 2016 to collaborate on a range of cyber issues, including holding a trans-Tasman cyber incident exercise as a part of the Australia – New Zealand cyber dialogue expected to take place in the second half of 2017. More action is needed to achieve this outcome.	

Action	Outcome	Progress to date	Rating
RAISE THE BAR			
13. 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 cyber awareness campaign, Stay Smart Online, has published a range of guides on cybersecurity. The development of the *Security awareness implementation guide*, the *Small business guide*, and *My guide* for individuals in partnership with New Zealand and the private sector (Australia Post, ANZ, CBA, NBN Co, NAB, Westpac and Telstra) has increased the amount of cybersecurity guidance available for business and consumers. Note that Stay Smart Online was originally housed within the Department of Communications and the Arts, but is now the responsibility of the Attorney-General's Department.	
	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	This is intended to be a by-product of success on a preceding initiative, so it's presumed to be on track but requiring attention to ensure delivery.	
	Australian businesses, small and large, have improved understanding of good cyber security practices	This is intended to be a by-product of success on a preceding initiative, so it's presumed to be on track but requiring attention to ensure delivery.	
	Governments, critical services and high risk sectors demonstrate good cyber security practices	The establishment of the new Critical Infrastructure Centre in the Attorney-General's Department may have a positive impact on cybersecurity in the future, but no evidence to that effect is currently available.	
14. 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	ASD updated its Top 4 strategies to mitigate cyber incidents to become the Essential 8 in February 2017.	

Action	Outcome	Progress to date	Rating
15. Co-design voluntary cyber security 'health checks' for ASX 100 listed businesses	Executives and boards in the ASX 100 better understand cyber security strengths and opportunities for their business	ASIC and the ASX launched cybersecurity health checks for ASX 100 companies in November 2016. The ASX released its Cyber Health Check Report in April 2017, an industry led survey on cyber security governance in Australia's largest companies.	
	Decision makers in the ASX 100 receive tailored information on the impact of cyber risks to their companies	Progress of the ASX 100 and ASIC cybersecurity health checks, and increasing awareness at the board level of cyber threats, are positive signs of progress towards the achievement of this outcome.	
	Australia's highest performing businesses lead a national effort towards best practice cyber security	While there's greater awareness of cyber threats among the largest companies, their advocacy for best practice among small to medium enterprises is just beginning.	
	Increased cyber resilience in Australia's largest companies	The success of action towards this outcome is difficult to assess over the timeframe, but the involvement of the ASX 100 in health checks is a positive indicator of progress.	
16. 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	The Department of Industry, Innovation and Science's Cyber Security Small Business Program states intentions to provide a grant to CREST ANZ to increase its number of accredited service providers. The government advises that there's an ongoing information exchange of lessons from New Zealand's Cyber Credentials scheme; however, there's no evidence of the implementation of solid steps towards this outcome, so it's rated 'not commenced'.	
	CREST Australia New Zealand diversifies the services it accredits. Types of assessment might include penetration testing, vulnerability analysis and assessment against best practice standards	The Department of Industry, Innovation and Science's Cyber Security Small Business Program states intentions to provide a grant to CREST ANZ to diversify its services to include the accreditation of skills and capabilities. However, there's no evidence of implementation of this plan yet, so it's deemed 'not commenced'.	

Action	Outcome	Progress to date	Rating
17. 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	The Department of Industry, Innovation and Science's Cyber Security Small Business Program involves a grant for small businesses to have their cybersecurity tested by service providers approved by CREST ANZ. Grants of up to $2,100 in co-funding will be available on a one-off basis. Applications are expected to open in 2017–18 for grant payments to be made 2018–19.	
	Australian small businesses understand their potential cyber security vulnerabilities and where to find trusted cyber security advice	The delivery of the preceding three outcomes may lead to the achievement of this one, but data should be collected to ensure that its achievement is quantifiable.	
	Australian small businesses are empowered with the knowledge they need to make considered cyber security investments to protect their business long term	Government has facilitated greater access to cybersecurity knowledge for small businesses through the Stay Smart Online *Small business guide* and *Security awareness implementation guide*. Minister Dan Tehan's March business roundtable focused on small to medium enterprises, and the Department of Industry, Innovation and Science plans to offer small business grants for CREST ANZ accredited cybersecurity. However, the general stakeholder perception is that there's still an urgent need for the government to engage more effectively with small businesses on cyber issues. Data collection through methods such as sentiment surveys of business needs to be commenced now to ensure that progress towards this outcome is quantifiable.	
	Large and small businesses increase trust in the connections they have with each other	The achievement of this outcome is challenging to judge objectively, and it's unclear how this is related to the action of security testing by CREST-accredited service providers.	

Action	Outcome	Progress to date	Rating
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	Government agency cyber security practices are the exemplar for public and private sector organisations in Australia	ASD has conducted surveys of Commonwealth agencies cyber security based on implementation of the 'Top 4' strategies to mitigate targeted cyber security incidents. However ANAO audits of several departments and a survey of government agency cybersecurity practice by the Australian National University's National Security College indicate that there's significant work to be done to achieve this outcome, and that some agencies are failing to fully implement the Top 4 strategies. Therefore, government agencies are off track to win the title of 'exemplar' in this space.	
	Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability	Government agencies have access to cybersecurity advice from ASD, including ASD's strategies to mitigate cyber security incidents and *Information security manual*. However, the implementation of better cybersecurity practice in government agencies requires their own skilled staff, adequate financial resources and commitment from senior executives to act on cybersecurity advice from responsible agencies. The establishment of a new Cyber Security Advisory Office within the DTA was announced in the 2017-18 Budget to provide cybersecurity advice on government IT procurement.	
	Non-Government information stored on Government networks is resilient to malicious cyber activity	While this is difficult to assess at the whole-of-government level, the ANAO audit of the Australian Taxation Office and the Department of Immigration and Border Protection, and the 2015 Bureau of Meteorology hack, indicate that significant work is needed to achieve this outcome.	

Action	Outcome	Progress to date	Rating
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	Government agency cyber security practices are the exemplar for public and private sector organisations in Australia	The Annual Update notes that ASD has conducted surveys of Commonwealth agencies cyber security based on implementation of the 'Top 4' strategies to mitigate targeted cyber security incidents. Government has previously advised that pilot program was planned to begin in 2018–20. Being an exemplar of cybersecurity is a lofty goal for any sector, particularly a large and diffuse organisation such as the Australian government. While the ANAO's cybersecurity audits of government departments indicate a pleasing interest in ensuring that the government is setting a good example, the audit results and a survey of government agency cybersecurity practices by the National Security College indicate that there's significant work to be done to achieve this ambitious outcome.	
	Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability	Government agencies have access to advice from ASD, but the implementation of better cybersecurity practice requires skilled staff, adequate financial resources and commitment from senior executives to act on cybersecurity advice from responsible agencies.	
	Non Government information stored on Government networks is resilient to malicious cyber activity	While this is difficult to assess at the whole-of-government level, the ANAO's audit of the Australian Taxation Office and the Department of Immigration and Border Protection indicates that significant work is needed to achieve this outcome.	
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	Government agency cyber security practices are the exemplar for public and private sector organisations in Australia	ANAO audits of several departments and a survey of government agency cybersecurity practice by the National Security College indicate that significant is needed to achieve this outcome.	
	Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability	Government agencies have access to advice from ASD, but the implementation of better cybersecurity practice requires skilled staff, adequate financial resources and commitment from senior executives to act on cybersecurity advice from responsible agencies	
	Non Government information stored on Government networks is resilient to malicious cyber activity	While this is difficult to assess at the whole-of-government level, the ANAO audit of the Australian Taxation Office and the Department of Immigration and Border Protection indicates that significant work is needed to achieve this outcome.	
21. 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	The Annual Update notes that work on this has not yet commenced.	

GLOBAL RESPONSIBILITY AND INFLUENCE

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

Action	Outcome	Progress to date	Rating
22. Appoint a Cyber Ambassador	Australia has a coordinated, consistent and influential voice on international cyber issues	Dr Tobias Feakin's appointment as Ambassador for Cyber Affairs was announced on 10 November 2016, and he took up his post on 3 January 2017. The delay in appointing Dr Feakin to this role means that, while progress towards achieving an influential international voice on cyber issues for Australia is being made, it can't yet be considered complete. Publishing the expected International Cyber Engagement Strategy will be an important way of achieving this outcome.	
23. Publish an international engagement strategy on cyber security	Australia's international engagement on cyber issues is prioritised and coordinated	Work has commenced within DFAT on the International Cyber Engagement Strategy. The department completed the first round of international and whole-of-government consultations and opened public submissions for the strategy until 31 March. Publishing the International Cyber Engagement Strategy, expected later in 2017, will be an important way of achieving this outcome.	
	Stakeholders understand Australia's position on key cyber issues being debated on the world stage	This outcome is reliant on achieving coordination and a consistent voice on these issues and a clear strategy.	
24. 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	Australia has been an active participant in the current round of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which discusses cyber norms and confidence building measures. Australia continues to advocate for open, free and secure access to cyberspace and the multistakeholder model of internet governance in relevant international forums. Australia is a member of the Freedom Online Coalition and engages in resolutions relating to internet freedoms in the Human Rights Council and UN General Assembly Third Committee. Australia has engaged bilaterally with international partners to discuss cybersecurity, including in the Japan–Australia Cyber Policy Dialogue held in August 2016 and the Australia–China Cyber Policy Dialogue in February 2016. Australia also held the chair of APCERT in 2016.	

Action	Outcome	Progress to date	Rating
25. 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.	Australia has announced increased cooperation with Indonesia through the Ministerial Council on Law and Security, but more action towards this outcome is needed to achieve the objective.	
	International efforts to prosecute cybercrime are enhanced	Australia engages internationally from multiple departments to shut down cybercrime safe havens. The Attorney-General's Department helps Pacific island countries tackle cybercrime through the Pacific Islands Law Officer's Network, CERT Australia offers training to other CERTs in the region, and the AFP's Cyber Safety Pasifika Program raises awareness on cybercrime issues in Pacific island countries. The government advises that DFAT partnered with the UN Office on Drugs and Crime in 2016 to fund a training course for cybercrime investigators and prosecutors in Southeast Asia. AFP Cybercrime liaison officers and Australian Criminal Intelligence Commission cybercrime analysts are posted in Washington DC and London. Australia has recently increased international efforts to cooperate on cybercrime through pressing the issue with Indonesia at the Ministerial Council on Law and Security meeting. The meeting has been held in December 2015, July 2016 and most recently in February 2017. This is a good step in the right direction, but more action to this effect will be needed for this outcome to be considered 'on track'.	
26. 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	This is an ongoing effort that government agencies were engaged in before the Cyber Security Strategy, and it's difficult to assess the efficacy of these ongoing activities in the 12 months since the strategy was released. Releasing an International Cyber Engagement Strategy that takes a strong vision on Australia's contribution to this issue and the necessary coordination will ensure that this outcome is achieved. DFAT has sought proposals from external organisations to undertake capacity building efforts in the Asia–Pacific through the new Cyber Cooperation Program, which has been funded with $1 million per year over four years. Other efforts include sponsoring the attendance of officials from Samoa, Vanuatu, Cambodia, Indonesia, Papua New Guinea, Myanmar, Vietnam, Thailand and Fiji at the Australian Cyber Security Centre conference in March 2017. The government has also advised that cyber workshops run by ICT4Peace, an NGO, were hosted in Hanoi and Vientiane for diplomats, officials and academics from Cambodia, Laos, Myanmar and Vietnam in 2016 and 2017. The government is also looking to fund cyber officials from Pacific islands to attend the Pacific Island Law Officers Network on Cyber Crime and the Pacific Cyber Workshop, which are to be hosted by Australia, the US and Japan in Tonga during May 2017.	

GROWTH AND INNOVATION

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

Action	Outcome	Progress to date	Rating
27. 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	The Australian Cyber Security Growth Network (ACSGN) was established on 5 December 2016 under the leadership of former Atlassian executive Craig Davies. Austrade has supported a group of 26 Australian cybersecurity organisations to attend the RSA Conference in the US, led by Mr Davies, and released the *Cyber security industry capability report* highlighting the capabilities of Australia's cybersecurity industry to foreign investors. ACSGN has also released a *Cyber Security Sector Competitiveness Plan*. The report, developed in conjunction with AlphaBeta is intended to help Australia's cybersecurity industry 'reach its full potential' by identifying and overcoming roadblocks to small business, commercialisation of research and a cyber skilled workforce.	
	More cyber security start-ups acquire capital to establish	While there have been promising steps, such as the Future Fund's investment in Bitglass, there remains a perception that Australian cyber start-ups must travel to the US or elsewhere to obtain the necessary capital for growth.	
	More cyber security solutions are developed and commercialised	There's insufficient baseline information available to quantify any increase in the commercialisation of Australian cybersecurity solutions. Action should be taken to collect the information needed to measure the growth of the industry. This outcome is dependent on the successful expansion and operation of the ACSGN.	
	The number of cyber security businesses in Australia grows	There's insufficient baseline information available to quantify any increase in the numbers of Australian cybersecurity businesses. Action should be taken to collect the information needed to measure the growth of the industry. This outcome is dependent on the successful expansion and operation of the ACSGN.	
	More Australian cyber security products and services are exported	The baseline against which this indicator is to be measured is not available, and no information against which success or failure can be judged is yet available. This outcome is dependent on the successful expansion and operation of the ACSGN.	
	More international businesses invest in Australian cyber security research, innovation and solutions	While there's no baseline data available to assess an increase, Austrade has reported significant foreign investment activity. This outcome is dependent on the successful expansion and operation of the ACSGN.	
	All businesses benefit from cyber security solutions commercialised with Growth Centre support	It isn't clear how progress towards this outcome can be measured.	

Action	Outcome	Progress to date	Rating
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	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	As the ACSGN has been operating only since December, it's difficult to perceive significant progress against this outcome. However, cooperation between the ACSGN and Data61 appears to be progressing. Data61 has been allocated a substantial budget, but it's unclear specifically what it will be spent on. The Department of Industry, Innovation and Science has established a 'digital market place' as part of the NISA, where small companies can engage to increase their profile for government procurement contracts.	
	The number of students in cyber security PhD programs increase, through the support of Data61 scholarship programs	No data on the number of PhD students against which to measure any increase in their number is available. However, Data61 does have 40 PhD students with a specific focus on cybersecurity issues, and the current scholarship round includes 12 new cyber focussed PhD offers.	
	SINET is successfully established in Australia bringing together cyber innovators, buyers and investors, complementing activities of the Cyber Security Growth Centre	The first SINET61 conference was held in Sydney in September 2016, and the second will be held in September 2017.	
29. 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	The Annual Update notes efforts to increase partnerships between industry and academic institutions, such as the Oceania Cyber Security Centre in Victoria, Commonwealth Bank and UNSW, and Optus and Macquarie University in Sydney. However it is not apparent that these partnerships have increased the coordination or competitiveness of Australian cyber R&D.	
	Australia's cyber security R&D explores current and emerging challenges for Australia's national cyber security	In March 2017 the Department of Defence announced the Next Generation Technologies Fund, which is intended to facilitate research partnerships between Data61 and Australian universities to address emerging cyber threats. The success of this initiative cannot be assessed as it has only just begun.	
30. 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	Initiatives such as Austrade's *Cyber security industry capability report*, highlighting the capabilities of Australia's cybersecurity industry to foreign investors, indicate that there's significant activity towards this objective, but more work is needed for their understanding to be considered mature.	
	The Government invests in developing Australian-based cyber security ideas	Initiatives such as funding for Australian delegations at the RSA Conference and the cybersecurity delegation that visited the US for Australia–US Business Week in August 2016 are encouraging signs of progress. Future Fund investment in cybersecurity firms is a promising sign, but further evidence of government investment is needed to ensure action towards the achievement of this outcome. Austrade's establishment of Australian innovation 'landing pads' in Berlin, San Francisco, Shanghai, Singapore and Tel Aviv is also helping to support the maturation of Australian start-ups.	
	More international organisations invest in Australia and the Australian cyber security sector	While no baseline data to assess an increase is available, Austrade has reported significant foreign investment activity.	

A CYBER SMART NATION

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

Action	Outcome	Progress to date	Rating
31. 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	In February 2017, the Minister for Education, Senator Simon Birmingham, and the Minister Assisting the Prime Minister on Cyber Security, Dan Tehan, announced that applications would be accepted from universities seeking to be recognised as cyber academic centres of excellence. The Annual Update notes that the successful institutions will be announced in 2017. This program has a total budget of $1.9 million over four years (to 2020), or $475,000 per year. There has also been strong private sector activity in this space, including CBA's partnership with UNSW and Optus's collaboration with Macquarie University. Despite those activities, it's not clear how progress towards this outcome can be practically measured.	
	The number of cyber security graduates increases	Several new cybersecurity courses have been launched by Australian universities in the past 12 months. However, there's no information available publicly on how many cybersecurity graduates there are in Australia, so it isn't possible to assess whether there has been an increase in numbers. Again, private-sector efforts to co-design and support cybersecurity courses are making headway on this issue.	
	The number of children studying subjects at school that will equip them for careers in cyber security increases	The 'Young Australians' program of the NISA is promoting digital literacy in primary school and students' take-up of STEM classes in high school, ASD has pushed a high school recruitment drive for short-term student placements, and bottom-up changes are occurring in school curriculums and extracurricular programs. However, the absence of research data on how many Australian students were equipped for careers in cybersecurity 12 months ago makes improvement in this area hard to judge.	

Action	Outcome	Progress to date	Rating
	More women and people with diverse backgrounds take up and change to a career in cyber security	While there's no baseline data available to assess any increase in the diversity of the cyber workforce, there is an active program of engagement with women in the industry to understand barriers to participation and provide solutions. To date these initiates are focussed on increasing female participation in the cyber workforce, and there is no evidence of work to address boarder diversity issues. For example, a 'women in cyber' lunch was held in Melbourne on International Women's Day 2017, last year the female participants of the 2015 Australian Cyber Security Challenge were offered a special program of events and mentorship, and the ACSC held a women's networking event for female technical practitioners. These actions are a positive influence, but it will take considerable time before they translate into women making career changes. Also, focusing on technical skills will solve only part of the problem. There's a need to attract individuals from a broader range of disciplines, including policy, communications and law, to achieve a truly diverse cyber workforce.	
	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	Initiatives such as Stay Smart Online week and increasing numbers of university courses suggest that the opportunity to improve cybersecurity knowledge is available, but there's no data on how many people have taken up that opportunity. Data61 and the Australian Institute of Company Directors began working together in April 2016 to elevate the level of cyber literacy of directors and boards across Australia. Data61 CEO Adrian Turner hosted an educational webinar on cyber incident management in November 2016 for 440 members of the institute. However, the curriculum still appears to be in the development stage, and greater speed of delivery will be needed for this outcome to be achieved. .	
	Opportunities to participate in Australian cyber security competitions increases, including internationally	The Cyber Security Challenge Australia remains the only national level competition. ASD has begun a high school level competition, which recently featured a coding day for female students in Canberra schools, and La Trobe University has partnered with Cisco and Optus to hold Cyber Games for Melbourne high school students. However, more evidence of support for participation in international competitions, and more frequent competitions in Australia, would be needed for the achievement of this outcome.	
32. 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	Achievement of this outcome is difficult to measure, but there's ongoing growth in the exchange of information between the public and private sectors, including sharing of corporate and government information and awareness programs.	
33. 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	Australia's cyber awareness raising campaign, Stay Smart Online, was held in coordination with Cyber Security Awareness Month in the US. Stay Smart Online reports new information-sharing arrangements with international partners, including the US, New Zealand and the UK. Australia's Stay Smart online also collaborated with New Zealand's Connect Smart awareness initiative, as well as the private sector, to co-develop the *Security awareness implementation guide* for businesses in October 2016.	

APPENDIX 2: HOW MUCH IS THE AUSTRALIAN GOVERNMENT SPENDING ON CYBER ISSUES?

The cross-portfolio nature of cyber issues and a lack of definition about what is 'cyber' expenditure make it difficult to parse the true extent of the overall Australian Government cyber budget. Major policy announcements such as the Cyber Security Strategy, but also the National Innovation and Science Agenda and the 2016 Defence White Paper, all include expenditure that can be related to the cybersecurity objectives of the strategy. This funding is distributed across several agencies and departments, increasing the opacity of the financial resources government has committed to achieve its objectives for cybersecurity. The analysis in this appendix attempts to break the funding commitments down using information available in the 2016–17 and 2017–18 Budget, and the 2015–16 and 2016–17 Mid-Year Economic and Fiscal Outlooks (MYEFOs) to determine the extent of new Australian Government cyber funding. Existing funding for cyber-related activities by agencies is even more difficult to discern. The tables below discuss new appropriations, except where the use of existing funds has been explicitly mentioned in policy documents and announcements.

When budget commitments above existing baseline funding for initiatives related to achievement of the objectives outlined in the Cyber Security Strategy, including those funded under the NISA and the Defence White Paper, are amalgamated, government has budgeted to spend $493.9 million between 2015–16 and 2019–20. These funds are largely funding the efforts of the Attorney-General's Department, Data61 and the Department of Innovation and Science. While Defence was promised an additional $300–400 million out to 2026 in the Defence White Paper, when that funding is spread evenly over 10 years, and transfers of appropriation to other departments are included, new funding to Defence out to 2019–20 dips below $40 million. Most the new funding doesn't begin until 2018–19, suggesting that departments and agencies have been given a two-year lead time to prepare for the beginning of new cyber initiatives. While it's reasonable for agencies to be given some time to prepare, two years for a priority issue is very generous for programs with no capital component, such as awareness-raising and education programs.

A regular update from government on its expenditure and future budgets for cyber issues, perhaps as part of regular annual reviews of cyber policy and strategy, would be a significant step towards tracking the achievement of cybersecurity goals. It would also provide a baseline from which to assess Australian expenditure against regional and other countries to ensure that investment is reasonable and adequate to meet emerging challenges. It may also give the government the opportunity to better understand areas of duplication or gaps in its strategy and provide private-sector partners with surety of continuity of programs that they may invest their own funds in implementing.

Table 2 compiles the NISA programs that are related to achieving the government's cybersecurity goals from the 2015–16 MYEFO. These programs, totalling $356.6 million over five years, are either directly related to cybersecurity or have a significant relationship with the achievement of the government's Cyber Security Strategy objectives by supporting the growth of Australian cyber skills and industry. This includes $74.6 million for CSIRO's Data61, far beyond the $7.5 million noted as earmarked by NISA for Data61 in the Cyber Security Strategy funding table. A small portion of this funding comes directly from PM&C, and is noteworthy as the only funding allocated to PM&C anywhere for the implementation of cyber-related activities.

TABLE 2: 2015–16 MYEFO

Expense ($m)	2015–16	2016–17	2017–18	2018–19	2019–20	Total
CSIRO—Data61	0	24.2	24.4	24.5	0	**73.1**
Department of Industry, Innovation and Science	26.6	27.7	25.8	36.3	0	**116.4**
NISA—Advancing Australia's cyber security	0	4.2	6.8	10.8	0	**21.8**
NISA—Innovation and Science Australia	1.1	2.3	2.5	2.3	0	**8.2**
NISA—Inspiring all Australians in STEM	25.5	13.2	8.7	15.5	0	**62.9**
NISA—Quantum computing	0	5.4	5	5	0	**15.4**
NISA—Supporting incubators	0	2.6	2.8	2.7	0	**8.1**
Department of Education and Training[a]	0	14.9	16.5	17.8	0	**49.2**
Department of the Prime Minister and Cabinet[b]	0	0.5	0.5	0.5	0	**1.5**
Total	**53.2**	**95**	**93**	**115.4**	**0**	**356.6**

a NISA: Inspiring all Australians in STEM.
b NISA: Data61.

When the government released the Cyber Security Strategy, it noted that 'about' $230 million would be allocated over four years to fund the actions initiated by the strategy. The funding table provided by PM&C notes that at least $38 million of that amount had previously been announced as part of the government's $1.1 billion National Innovation and Science Agenda, released in December 2015.[17] Additionally, the 2016 Defence White Paper indicated that Defence would spend $300–400 million over 10 years on expanding its cybersecurity capabilities.

Funding of $195 million over four years for strategy initiatives was appropriated in the 2016–17 Budget. Table 3 makes it clear that, while the strategy is certainly funded, a significant proportion of the budget is actually reappropriated Defence funding rather than new funding. Defence has transferred $122 million to several other departments and agencies and has not been allocated additional appropriation for the $51 million of strategy initiatives that it's responsible for implementing.

Once the transfer of appropriation from Defence is taken into account, new funding for strategy initiatives in 2016–17 and 2017–18 is $0.4 million and $0.2 million, respectively, before ramping up to $5.4 million of new funding in 2018–19. This suggests that funding has been phased to account for expected delays in implementation while agencies develop capacity to deliver the initiatives. In total, the government has to find only an additional $14.2 million over four years to fund the strategy's implementation, of which $13.6 million doesn't need to be found until the later years of the estimates.

Despite being given a significant leadership role in the delivery of the Cyber Security Strategy, PM&C hasn't received any additional funding over the forward estimates for strategy implementation. The Department of Communications and the Arts plays a key role in pursuing Australia's international cyber objectives through its work in bodies such as the International Telecommunication Union, but has also received no additional funding. Similarly, DFAT will meet its strategy commitments from existing funding, and no new funding has been appropriated.

17 https://cybersecuritystrategy.dpmc.gov.au/assets/img/Cyber-Security-Strategy-Funding-fact-sheet.docx

The far right column of Table 3 shows the difference between funding announced in the Cyber Security Strategy and funding provided in the Budget. While most agencies were appropriated the funding promised in the strategy, it's clear that most of the funding is redistributed or rebadged existing funding and, as noted above, most of this has come out of the Defence budget.

TABLE 3: 2016–17 BUDGET—CYBER SECURITY — IMPLEMENTATION OF AUSTRALIA'S CYBER SECURITY STRATEGY

							Funding announced in strategy	Difference between strategy funding and 16–17 Budget
($m)	**2015–16**	**2016–17**	**2017–18**	**2018–19**	**2019–20**	**Total**	**($m over four years)**	**($m over four years)**
Attorney-General's Department	0.0	16.5	22.5	22.0	21.3	**82.3**	82.4	–0.1
Expense	0.0	12.8	17.4	17.3	18.3	**65.8**		
Capital	0.0	3.7	5.1	4.7	3.0	**16.5**		
Australian Federal Police	0.0	4.1	5.5	5.4	5.4	**20.4**	20.4	0.0
Expense	0.0	3.1	5.3	5.4	5.4	**19.2**		
Capital	0.0	1.0	0.2	0.0	0.0	**1.2**		
Australian Criminal Intelligence Commission	0.0	1.7	4.8	4.4	4.4	**15.3**	16	–0.7
Expense	0.0	1.7	4.8	4.4	4.4	**15.3**		
Capital	0.0	0.3	0.4	0.0	0.0	**0.7**		
Department of Defence	0.0	–23.5	–34.0	–32.6	–32.0	**–122.1**	51.1	–173.2
Capital	0.0	–23.5	–34.0	–32.6	–32.0	**–122.1**		
Department of Education and Training	0.0	0.9	0.8	0.8	0.9	**3.4**	3.5	–0.1
Department of Industry, Innovation and Science[a]	0.0	0.7	0.6	5.4	8.2	**14.9**	15	–0.1
Department of the Prime Minister and Cabinet	0.0	0.0	0.0	0.0	0.0	**0.0**	0.0	0.0
Department of Communications and the Arts	0.0	0.0	0.0	0.0	0.0	**0.0**	0.0	0.0
Department of Foreign Affairs and Trade	0.0	0.0	0.0	0.0	0.0	**0.0**	6.7	–6.7
Total[b]	**0.0**	**0.4**	**0.2**	**5.4**	**8.2**	**14.2**	**195.1**	**–180.9**

a Does not include $30.5 million announced under NISA.
b Does not include $30.5 million announced under NISA for Innovation and $7.5 million for CSIRO also announced under NISA.

Two further cyber-related initiatives were announced in the 2016–17 MYEFO: additional support for women and girls in STEM and an expansion of incubator support of innovative new businesses (Table 4). These two initiatives add a further $46.4 million to cyber-related funding out to 2019–20.

TABLE 4: 2016–17 MYEFO

Expense ($m)	2015–16	2016–17	2017–18	2018–19	2019–20	Total
Department of Education and Training[a]	0.0	2.8	8.1	9.7	10.6	**31.2**
Department of Industry, Innovation and Science[b]	0.0	3.8	3.8	3.8	3.8	**15.2**
Total	**0.0**	**6.6**	**11.9**	**13.5**	**14.4**	**46.4**

a Supporting Women and Girls in STEM.
b Incubator Support for Innovative New Businesses and Jobs—expansion.

TABLE 5: 2017–18 BUDGET

Expense ($m)	2016–17	2017–18	2018–19	2019–20	2020–21	Total
Digital Transformation Agency	0	2.8	2.7	2.6	2.6	**10.7**
Cyber Security Advisory Office	0	2.8	2.7	2.6	2.6	**10.7**
Bureau of Meteorology —improved security and resilience	0	0.2	0	0	0	**0.2**
Total	**0**	**3**	**2.7**	**2.6**	**2.6**	**10.9**

The 2017–18 Budget included additional funding for a new Cyber Security Advisory Office (CSAO) within the Digital Transformation Agency (DTA), part of the Department of the Prime Minister and Cabinet. The CSAO's establishment is the government's response to recommendations stemming from #censusfail to improve the quality and coordination of cybersecurity advice to government agencies on information technology projects. DTA was also provided an additional $200,000 for cybersecurity improvements at the Bureau of Meteorology following that agency's significant cybersecurity breach reported in 2015.

TABLE 6: TOTAL BUDGETED EXPENDITURE, 2015–16 TO 2019–20

Expense and capital ($m)	2015–16	2016–17	2017–18	2018–19	2019–20	Total
Attorney General's Department	0.0	16.5	22.5	22.0	21.3	**82.3**
Australian Federal Police	0.0	4.1	5.5	5.4	5.4	**20.4**
Australian Criminal Intelligence Commission	0.0	1.7	4.8	4.4	4.4	**15.3**
Department of Defence	0.0	16.5	6.0	7.4	8.0	**37.9**
2016–17 Budget	*0.0*	*–23.5*	*–34.0*	*–32.6*	*–32.0*	*–122.1*
2016 Defence White Paper[a]	*0.0*	*40.0*	*40.0*	*40.0*	*40.0*	*160.0*
Department of Education and Training	0.0	18.6	25.4	28.3	11.5	**83.8**
Department of Industry, Innovation and Science	26.6	32.2	30.2	45.5	30.1	**164.6**
Department of Communications and the Arts	0.0	0.0	0.0	0.0	0.0	**0.0**
Department of Foreign Affairs and Trade[b]	0.0	1.7	1.7	1.7	1.7	**6.7**
Digital Transformation Agency[c]	0	0	3.0	2.7	2.6	**8.3**
Data61	0	24.7	24.9	25	0	**74.6**
CSIRO	*0*	*24.2*	*24.4*	*24.5*	*0*	*73.1*
Department of the Prime Minister and Cabinet	*0*	*0.5*	*0.5*	*0.5*	*0*	*1.5*
Total	**26.6**	**116.0**	**124.0**	**142.4**	**85.0**	**493.9**

a Assumes 2016 Defence White Paper Funding distributed evenly over 10 years.
b Assumes even distribution of internal funding.
c Does not include 2020–21 funding from 2017–18 Budget.

Table 6 aggregates the funding from the 2015–16 MYEFO, the 2016–17 Budget and MYEFO, 2017–18 Budget, and estimated funding provided under the Defence White Paper for an expansion of Defence's cyber capability ($300–400 million over 10 years) and internal funding from DFAT for the Cyber Ambassador position and capacity building activities of $6.7 million over four years. This shows that, when the Cyber Security Strategy's programs are combined with programs funded under the NISA and the Defence White Paper that are related to the achievement of the government's cybersecurity objectives, the government has committed new funding of over $493.9 million over five years to cybersecurity issues.

The largest amount ($164 million over four years) is administered by the Department of Industry, Innovation and Science as part of NISA programs. The Attorney-General's Department ($82.3 million) and the Department of Education and Training ($83.8 million) are also managing sizeable cyber-related budgets. When compared to the allocations for these large line departments, the $74.6 million allocated to Data61 is an impressive sum for the agency.

ACRONYMS AND ABBREVIATIONS

ACSC	Australian Cyber Security Centre
ACSGN	Australian Cyber Security Growth Network
AFP	Australian Federal Police
ANAO	Australian National Audit Office
ASD	Australian Signals Directorate
CSAO	Cyber Security Advisory Office
DFAT	Department of Foreign Affairs and Trade
DTA	Digital Transformation Agency
JCSC	Joint Cyber Security Centre
MYEFO	MidYear Economic and Fiscal Outlook
NISA	National Innovation and Science Agenda
PM&C	Department of the Prime Minister and Cabinet
STEM	science, technology, engineering and mathematics

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

ASPI

Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au
Blog www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC
www.aspi.org.au/icpc/home


ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE
INTERNATIONAL
CYBER POLICY
CENTRE