TELSTRA CORPORATION LIMITED

Australia's 2020 Cyber Security Strategy

Public submission

8 November 2019

CONTENTS

EXECUTIVE SUMMARY

At Telstra, we believe a digital economy built on a secure foundation is key to generating trust and confidence in the products and services that connect us all. Critical infrastructure providers, including telecommunications and internet service providers, depend on the stable and secure functioning of the internet to deliver essential services to populations around the globe. Building this secure foundation is a shared responsibility for governments, the private sector and the community.

Telstra is proud to assist our customers in improving and securing the ways in which they live and work. Given our place in Australia's telecommunications past, present and future, we recognise that our role does not stop at our own networks; we know we have an important role to play in supporting our nation to be cyber resilient. Because of this, Telstra has a long history of working alongside the Australian Government on both operational security and cyber policy issues.

Australia's 2016 Cyber Security Strategy established an important baseline of an 'Australian vision' for cyberspace and successfully established foundational structures and institutions to help us realise this vision. It is now time to build upon this groundwork, delivering further cyber security benefits for Australia's economy and society. This is the focus of our recommendations for the 2020 strategy.

We are strong proponents of evidence-based public policy that is grounded in a fundamental understanding of both technology and threat. Our submission is informed by the expertise of our people who hold industry-leading technical and policy knowledge in areas including foundational technologies, such as 5G, Cloud, artificial intelligence, as well as critical infrastructure protection, incident response, threat intelligence, national security, strategic policy, risk, cyber skills development, behavioural influence, customer education and diversity and inclusion.

Telstra commends the Australian Government for releasing *Australia's 2020 Cyber Security Strategy Discussion Paper*, which will facilitate an important dialogue on cooperation and implementing a shared vision for Australia's approach to cyberspace. We welcome the opportunity to contribute some of our insights on the key technology, policy and strategic issues facing the nation.

In summary, we recommend:

1. **Jointly assessing the cyber-threat environment:** Improved threat intelligence sharing through specific initiatives including co-locating government and industry practitioners and expertise to better address high impact cybercrime techniques targeting consumers.
2. **Government-industry partnering (strategic):** Establish formalised communication channels, reporting and forums with regular cadence between government and industry decision-makers to better inform operational and legislative priorities.
3. **Government-industry partnering (operational):** Improved governance and operational initiatives to strengthen the effectiveness of the Joint Cyber Security Centres (JCSCs) in collaborating with industry, including appointing a designated point of contact for Critical National Infrastructure (CNI) organisations and reviewing the classification of information to reduce barriers to information sharing.
4. **Policy co-operation:** Maintain transparency on offensive cyber capabilities and build closer cooperation with the private sector on international policy development and engagement. Government to develop and lead a national level cross-sector crisis response exercise with key industry sectors to inform policy.
5. **Building enterprise and skills, influencing behavioural change:** Government to use levers such as tax, immigration and business policies, and academic accreditation, to ensure robust cyber security talent pipelines. Consolidate efforts to raise awareness and influence consumers in developing strong cyber security behaviours.

Summary of Recommendations

Recommendations	
1.4.1.	Industry and government to form an expert group to agree priority network-level threats and together engage the most appropriate global forums for the promotion and adoption of security best practice to address these (e.g.: Mutually Agreed Norms for Routing Security (MANRS) for BGP).
1.4.2.	Industry and government to form Australian Cyber Security Centre (ACSC)-led cross-sector working groups to consolidate visibility of high-volume cybercrime impacting consumers, and identify existing capabilities, processes and legislative tools to address this threat.
1.4.3.	Industry to lead the development of best practice software standards to reduce impacts of potential attacks via mass market devices (e.g.: home automation, security cameras, drones, etc) leveraging existing standards such as the Internet of Things Alliance Australia's (IoTAA) *Internet of Things Security Guideline.* Government to endorse standards where appropriate to support wider adoption.
1.4.4.	Industry and government to form joint threat intelligence cells which co-locate practitioners within the JCSCs and/or ACSC, to focus on monitoring and countering new actors and techniques that are high-effort and high-impact.
2.5.1.	Government to undertake an annual national stocktake to quantify the scale and cost of cyber threats to Australia, share these insights publicly and use them to inspire evidence-based conclusions as to which programs may be making an impact on national resilience.
2.5.2.	Industry to repeat the ASX100 cyber health check with government support, improving on previous surveys by undertaking a split model approach and clarifying definitions of terms used.
2.5.3.	Government to establish a 2020 Cyber Security Strategy CEO industry advisory panel to provide input, advice and guidance on the ongoing implementation of the 2020 strategy initiatives.
2.5.4.	Government to re-establish previous regular quarterly operational meetings between the Minister responsible for cyber security and key industry CISOs. These meetings provided Ministers with front-line insights on key cyber security issues and opportunities for greater collaboration. Representation should cover key sectors including telecommunications, financial services, energy, healthcare, education and resources.
2.5.5.	Government and industry to consult on advanced threats to develop a risk- and threat-based collaborative response model.
2.5.6.	To ensure regulation is effective, Government to pursue consistency of obligations across providers of same services, whether or not traditionally licensed.
2.5.7.	Government to explore ways to adjust policy settings to help address technology challenges introduced by interdependencies with OTT providers.
3.4.1.	Industry to nominate issues of interest for discussion in advance of information exchange meetings (i.e.: country or vector) so that relevant Canberra-based experts can attend and provide more in-depth insights from a government perspective.
3.4.2.	Government to appoint a dedicated, visible, senior ACSC leader to be given responsibility for two-way engagement with CNI organisations on sensitive cyber security threats. This position would replace the current arrangements that often see industry advised to send sensitive information to a generic ACSC mailbox.
3.4.3.	Government to extend existing Slack groups to include industry verticals and/or thematic streams curated by ACSC sector/theme leads (e.g.: Open Source Intelligence, telco). These lead analysts promote discussion and collaboration and disseminate relevant, actionable information to the group.
3.4.4.	Government to lower the classification of information where possible and create more

	actionable advice for small businesses reflective to the size and capability of the organisations represented.
3.4.5.	Industry and Government to further enable cross-industry sharing by conducting an assessment on potential legislative barriers to sharing anonymised information e.g.: privacy legislation, and work together on solutions.
3.4.6.	Government to consider increased protections for information sharing not currently included in documents such as the ACSC Deed of Confidentiality. These could include protections from liability, regulation and civil actions, non-waiver of privilege, protection of intellectual property and confidentiality and protections from FOI requests.
3.4.7.	Government to establish a national governance framework to ensure consistency and connectivity across the JCSCs and with the ACSC, and to set clear national priorities to deliver programs of work in collaboration with industry.
3.4.8.	Government to increase empowerment of JCSCs and strengthen their local leadership.
3.4.9.	Industry JCSC Board/Steering Committee members to work with government to review and standardise a tiered engagement model.
3.4.10.	Trusted, long-term industry partners in the JCSCs to nominate trusted individuals within threat intelligence companies as a first step towards embedding approved vendors.
3.4.11.	Government to establish agreed day(s) for specific industries or practitioner roles to visit the JCSCs – like the Super Drop-In Day in Melbourne, which has been a positive experience.
3.4.12.	Government to share advice in advance of announcements and decisions that may impact industry, via the JCSCs (e.g.: attributing high-profile cyber-attacks to foreign governments).
4.4.1.	Government to provide an official, consistent definition as to what is considered 'critical infrastructure' in Australia, to better support policy cooperation with other Governments.
4.4.2.	Government to create a central, easily accessible location for the publication of policy positions and documents on the use of offensive cyber capabilities.
4.4.3.	Government to develop and lead regular national cross-sector crisis response exercises to test the national *Cyber Incident Management Arrangements* (CIMA). Specifically, scenarios exploring the *sustained disruption of essential systems and associated services, affecting CNI* and with *potential national security implications* would allow government and industry to establish mutual expectations and thresholds for a nationally-significant cyber crisis event. Running these exercises at a regular cadence e.g. annually would encourage continuous improvement, build strong partnerships and provide a mechanism for regular measurement of industry-wide cyber maturity.
4.4.4.	Where proper and appropriate, government to utilise the expertise that lies within Australian industry when engaging with international counterparts on cyber security issues.
5.4.1.	Government to use levers such as tax, immigration and business policies that incentivise investment, research and innovation to create a legislative and economic environment that supports growth in the cyber security talent pipeline and supply chain.
5.4.2.	Government and key industry partners such as Telstra to jointly map internal cyber security technical capabilities to categorise where existing capabilities lie across industry and government, how they could potentially be cross-utilised, and where skills gaps exist that need to be developed or sourced.
5.4.3.	Government to develop an accreditation scheme for cyber security higher education courses that is tied to the US National Initiative for Cybersecurity Education (NICE) framework, to ensure shared expectations of the skills taught in these courses and the job opportunities that match their qualifications.
5.4.4.	Government to promote a central, singular online brand identity (such as cyber.gov.au) for government cyber security messaging that delivers ongoing, engaging education initiatives in partnership with industry.
5.4.5	Industry and government to come together to perform a 'horizon-scan' of emerging

	technologies to identify both the opportunities and risks they present. This should look to leverage whole-of-government expertise and industry knowledge and seek to identify potential strategic security issues.
5.4.6	Cross-industry study involving major internet service providers (ISPs) to understand existing 'clean-pipes' initiatives and an exploration with government around potential commercial models that may deliver even greater upstream network protections to the Australian public.

01 Jointly Assessing the Cyber Threat Environment

As one of Australia's most important CNI providers, we recognise that the integrity and availability of Telstra's networks underpins the social and economic wellbeing of the nation. It is for this reason that Telstra continues to apply a national security lens to our operations and the cyber security of our networks.

We are observing an increase in online espionage, disruption and theft campaigns against industry targets in the Asia-Pacific and Australia. As the sophistication of cyber threats continues to evolve and the internet-connected IT surface expands exponentially, it's vital we understand not just how, but why our adversaries conduct malicious activities. Developing this level of understanding through our threat visibility and trusted networks allows Telstra to more effectively predict malicious activity and mitigate cyber risk.

Australian organisations hold a wealth of information desirable to threat actors. This includes data on the identity, location and behaviours of our customers, sensitive information about our networks and facilities, and valuable intellectual property on future technology and innovation.

We suggest three threat areas for increased focus over the near-medium term:

- Network-level threats
- High-volume cybercrime
- Emerging strategic cyber threats.

1.1. Network-level threats

Attack vectors exploiting weaknesses in how the internet itself functions, such as by subverting Border Gateway Protocol (BGP) and Domain Name System (DNS), are becoming increasingly prevalent. These risks can only be addressed effectively and at scale through global cooperation across networks and providers. However, the adoption of global best practice for network security can be difficult to achieve across countries with varying levels of ISP maturity and resourcing.

1.2. High-volume cybercrime

High-volume cybercrime attempts are generally untargeted and low in sophistication, but the sheer volumes deployed ensures an ongoing degree of profitability for cybercriminals.

Every day, Telstra uses a combination of DNS blacklisting and in-house technology to block an average of 23 million spam messages from being sent on our network. These messages, which represent 50-80% of the total number of emails sent per day, contain spam and potential malicious content or attachments. In addition to the direct financial costs to the consumer, successful high-volume cybercrime attacks can be time-consuming for cyber security professionals and law enforcement agencies to manage, diverting scarce resources away from more sophisticated threats.

1.3. Emerging strategic threats

In addition to high-volume, low-sophistication attacks, we are witnessing an increase in high-sophistication, high-impact attacks. As global connectivity increases, governments and organised criminals are increasingly realising the power of cyber capabilities to achieve political outcomes or criminal ends. Whilst traditional 'cyber power' countries continue to leverage previously unseen tactics, techniques and procedures, new emerging strategic actors are also utilising less-sophisticated, but still effective, exploitation techniques. This sees our national threat landscape continue to diversify.

1.4. Recommendations

1.4.1. Industry and government to form an expert group to agree priority network-level threats and together engage the most appropriate global forums for the promotion and adoption of security best practice to address these (e.g.: Mutually Agreed Norms for Routing Security (MANRS) for BGP).

1.4.2. Industry and government to form Australian Cyber Security Centre (ACSC)-led cross-sector working groups to consolidate visibility of high-volume cybercrime impacting consumers, and identify existing capabilities, processes and legislative tools to address this threat.

1.4.3. Industry to lead the development of best practice software standards to reduce impacts of potential attacks via mass market devices (e.g.: home automation, security cameras, drones, etc) leveraging

existing standards such as the Internet of Things Alliance Australia's (IoTAA) *Internet of Things Security Guideline.* Government to endorse standards where appropriate to support wider adoption.

1.4.4. Industry and government to form joint threat intelligence cells which co-locate practitioners within the JCSCs and/or ACSC, to focus on monitoring and countering new actors and techniques that are high-effort and high-impact.

02 Government-Industry Partnering (Strategic)

Meeting the challenge of keeping Australians safe online requires close engagement between government – which controls national and cyber security policy – and industry, which controls a significant proportion of communications networks, and where much of the technical innovation in cyber security takes place. Cyber security is a 'team sport' in which all organisations must do their best to protect their networks and customers from cyber threats. When industry and government work together, we can pool our resources and knowledge to help make Australia a harder target for malicious actors.

These partnerships can take the form of broad thematic work, e.g.: promoting best practice, influence and awareness amongst practitioners (like the Security Influence and Trust (SIT) Group), and on more targeted operational issues.[1] Partnerships that leverage the technical expertise and threat visibility found in industry and that are supported by effective legislative instruments generally result in the strongest outcomes for reducing cyber threat.

Details on the scale and cost of cyber threats to Australia often rely on data from self-reporting or international-focused sources. Drawing conclusions from data as to how industry should act, without Australia-specific threat information, can limit the effectiveness of even the best efforts to address cyber threat in the Australian environment.

Given the ACSC's 'whole of economy' remit, and to help better illuminate the current state of our threat environment, we believe a ground-up 'national stocktake' is required, using a more comprehensive range of data points. This stocktake should cover end users, small businesses and large companies, and where possible include data from existing law enforcement and government reporting, such as ScamWatch and the ACSC's recent Small Business Survey. Industry should advise on how best it can contribute anonymised and meaningful data. It is Australian businesses themselves that have the most coherent and detailed view of threats impacting their customers at scale. Industry and sector representative groups could be utilised to further this reach.

The *2016 ASX 100 Cyber Health Check* was an industry-led initiative and deliverable of the 2016 Cyber Security Strategy. The survey, which asked questions of the board members of ASX100 companies concerning organisational cyber security capability and risk, was an effective tool to initiate discussions on cyber security at the most senior levels.

The report identified five key trends:

1. Cyber security is a major and growing risk.
2. Tackling cyber risk needs a culture of collaboration.
3. Boards take cyber risk seriously and are improving their skills.
4. Companies are managing cyber risk better but realise there's still more to do.
5. Companies that manage cyber risk effectively define and analyse their exposure.

We believe it would be worthwhile repeating this survey to assess progress in the cyber maturity of Australia's largest organisations. A repeat survey may benefit from a 'split model approach' that would see strategic questions around risk and maturity directed to the board, and specific questions on technology stacks, controls and capabilities directed to Chief Information Security Officers (CISOs) and cyber security teams that are better placed to provide this detail. Increased clarity around the definition of key terms used in the survey (i.e.: attacked, incident and breach) will also assist with response baselining across organisations.

Cyber and national security briefings provided by senior government figures to private sector boards and executive committees have continued to be valuable. They have assisted to convey specific detail on the scale of the threat posed by advanced threat actors to Australian organisations. Ministerial engagement on cyber security with industry has also provided an effective mechanism for surfacing key issues facing private sector organisations.

[1] For example, the Scam Technology Project being led by the Australian Communications and Media Authority and the Australian Competition and Consumer Commission with assistance from the Australian Cyber Security Centre.

2.1. The regulatory environment

The telecommunications sector has a long and established relationship working with government on sensitive national issues. As such, we see a real opportunity to support government in identifying which components of our collaborative partnerships and regulatory engagements have worked well and utilising those learnings so that any wider harmonised model across sectors builds on a strong evidence-based foundation. We would also welcome the opportunity to work together to identify instances where we could standardise and refine existing legislation, in consideration of existing global frameworks and best practice such as NIST and the European Union National Information Systems Directive.

We acknowledge that there is inconsistent cyber security regulation across critical infrastructure sectors in Australia. Critical infrastructure sectors have many existing obligations under legislation including the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, the *Security of Critical Infrastructure Act 2018*, the *Telecommunications and Other Legislation Amendment Act 2017* (or Telecommunications Sector Security Reforms (TSSR) obligations) under the *Telecommunication Act 1997*, and additional rules and standards implemented by industry regulators.

As the telecommunications sector has most recently experienced through TSSR, the introduction of network- and facility-focused regulatory regimes provides a framework for industry and government to work together to identify and mitigate risks but can impose resource burdens and impact commercial decision-making timelines and outcomes. Organisations are required to meet these obligations in addition to compliance with the existing global standards by which cyber security teams already identify, assess and manage risk. Therefore, it is important to prioritise simplicity and harmonisation when considering additional legislative change.

2.2. Proactive identification of cyber risks

Commentary both within the discussion paper and elsewhere in the media[2,3,4] suggests that Government should have increased powers to intervene in industry networks without consent:

> Under existing legislative frameworks, government can only take direct action to prevent or respond to cyber security incidents with the permission of network owners (including other government agencies). This takes time and gives malicious actors an advantage. In national emergency situations, it may be appropriate for government agencies to take swifter action.[5]

We value and appreciate the deep technical expertise of government and understand that there are scenarios where it may be appropriate, and beneficial to industry, for government agencies to take swifter action.

In the context of the potential for a significant national cyber crisis response situation, government and industry should look to establish agreement between technical and leadership teams as to at what point an incident would reach a national security threshold, and the subsequent actions that could be taken, using existing legislative frameworks and Memoranda of Understanding. These models should be robust and regularly tested. A good international case study in this regard is the cooperation that took place between U.S. government agencies and U.S. banks during a significant DDoS campaign launched by Iranian government-aligned actors against U.S. financial institutions in 2012, in apparent retaliation for Western economic sanctions.

We appreciate the advantages greater visibility into the behaviour of critical networks could afford the government in better protecting national critical infrastructure. There are several different ways this could be achieved, with different levels of collaboration between agencies and network operators, and

---

[2] https://www.smh.com.au/politics/federal/intelligence-agency-could-be-used-for-offensive-cyber-operations-in-australia-20190614-p51xst.html
[3] https://www.itnews.com.au/news/dutton-drags-bank-cyber-into-asd-domestic-expansion-row-526821
[4] https://www.zdnet.com/article/australia-as-concerned-about-cyber-bond-villains-as-state-actors/
[5] Department of Home Affairs, *Australia's 2020 Cyber Security Strategy – A Call for views*, p10.

accordingly of technical and operational risks to the networks themselves. Industry can complement government expertise with its understanding of the complexities involved in managing and monitoring networks and operations, patching certain systems or remediating vulnerabilities at speed. Industry and government should explore options together and agree on the most effective solutions to proactively identify cyber risks.

2.3. Technology interdependencies

Many companies including Telstra hold a carrier or broadcast licence. These licences impose significant obligations and liabilities. If we do not meet those obligations, there are serious consequences. At the same time, many of the services we provide are increasingly mirrored by 'over-the-top' (OTT) providers who sit outside of our regulatory framework, including those who operate and broadcast over the internet instead of traditional channels and are not necessarily subject to the same obligations. To ensure that regulatory frameworks are effective to meet their objectives, it will be important to implement them using mechanisms that apply to all, not just traditionally licensed, providers of relevant services.

There are increasing interdependencies between network, communications, and OTT technology providers which need to be considered holistically when implementing cyber security. DNS over HTTPS is one example where implementation has effects across multiple types of providers and makes it much more challenging to provide security for our customers. The international experience has shown that sometimes these challenges need to be addressed using a combination of technology and policy levers. We would welcome consultation on national cyber security priorities that brings together network, communications and OTT technology providers to address end-to-end dependencies.

2.4. Organisational arrangements

Australia's Commonwealth cyber security frameworks have undergone multiple machinery of government changes over the past five years. Constant change can create uncertainty and instability both for industry, and for the public servants working to implement cyber strategy initiatives. We believe that now with the Australian Signals Directorate's (ASD) new whole-of-economy remit, the settings are close to ideal. We support current arrangements in preference to further centralisation of cyber security, cyber policy, or cyber safety functions in government.

2.5. Recommendations

2.5.1. Government to undertake an annual national stocktake to quantify the scale and cost of cyber threats to Australia, share these insights publicly and use them to inspire evidence-based conclusions as to which programs may be making an impact on national resilience.

2.5.2. Industry to repeat the ASX100 cyber health check with government support, improving on previous surveys by undertaking a split model approach and clarifying definitions of terms used.

2.5.3. Government to establish a 2020 Cyber Security Strategy CEO industry advisory panel to provide input, advice and guidance on the ongoing implementation of the 2020 strategy initiatives.

2.5.4. Government to re-establish previous regular quarterly operational meetings between the Minister responsible for cyber security and key industry CISOs. These meetings provide Ministers with front-line insights on key cyber security issues and opportunities for greater collaboration. Representation should cover key sectors including telecommunications, financial services, energy, healthcare, education and resources.

2.5.5. Government and industry to consult on advanced threats to develop a risk- and threat-based collaborative response model.

2.5.6. To ensure regulation is effective, Government to pursue consistency of obligations across providers of same services, whether or not traditionally licensed.

2.5.7. Government to explore ways to adjust policy settings to help address technology challenges introduced by interdependencies with OTT providers.

03 Government-Industry Partnering (Operational)

3.1. Information sharing

Challenges continue to face operational information sharing in Australia, due to a reliance on individual relationship-based sharing rather than more resilient operationalised arrangements. The Trusted Information Sharing Network (TISN) is not the most appropriate mechanism for sharing cyber threat information, and information flow from the ACSC on the threat landscape has not yet reached full maturity.

At a practitioner level, the National Information Exchange (NIE) and the more recent state-based efforts, (i.e.: the NSW Operational Intelligence Exchange (NOIE)) have proven to be useful forums to receive organisational updates from industry and government partners and gain some visibility of the threats facing the community. We suggest minor enhancements in our recommendations below.

3.2. Joint Cyber Security Centres

Telstra is a founding member of the Government's Joint Cyber Security Centre (JCSC) program, an initiative of the 2016 Cyber Security Strategy. We are active participants in the centre's activities and serve as members of the Sydney Steering Committee and Melbourne Interim Board. The JCSCs have made a significant contribution to improving Australia's national cyber resilience by creating communities of cyber security practitioners. However, much of the delivery has focused on events and one-off activities.

The JCSCs have untapped potential as a safe and trusted environment where operators of CNI and critical services can gather to discuss sensitive security issues or to coordinate response to significant incidents. However, uncertainty around how vendor presence is managed has occasionally impacted the ability or willingness of certain organisations to share in the JCSCs. A tiering model has previously been suggested in the JCSC context, to enable a wider range of participants in the centres while maintaining trust, this concept should be revisited.

3.3. Attribution

The Australian government, along with other nations, will now publicly attribute certain instances of malicious nation-state activity to specific countries. We welcome this activity and understand that it is undertaken to help reinforce appropriate norms of state behaviour online, including the norm that states must not intentionally damage or impair the use of critical infrastructure that provides services to the public. We also understand that some identified activity by nation-states may not be attributed by government for various reasons.

Following an attribution, there is some global precedent for large companies to be used as proxy targets in retaliation. A formal, advanced notification process to trusted CNI providers when attributions will take place would enhance the ability to monitor for and protect against this activity.

3.4. Recommendations

3.4.1. Industry to nominate issues of interest for discussion in advance of information exchange meetings (i.e.: country or vector) so that relevant Canberra-based experts can attend and provide more in-depth insights from a government perspective.

3.4.2. Government to appoint a dedicated, visible, senior ACSC leader to be given responsibility for two-way engagement with CNI organisations on sensitive cyber security threats. This position would replace the current arrangements that often see industry advised to send sensitive information to a generic ACSC mailbox.

3.4.3. Government to extend existing Slack groups to include industry verticals and/or thematic streams curated by ACSC sector/theme leads (e.g.: Open Source Intelligence, telco). These lead analysts promote discussion and collaboration and disseminate relevant, actionable information to the group.

3.4.4. Government to lower the classification of information where possible and create more actionable advice for small businesses reflective to the size and capability of the organisations represented.

3.4.5. Industry and Government to further enable cross-industry sharing by conducting an assessment on potential legislative barriers to sharing anonymised information e.g.: privacy legislation, and work together on solutions.

3.4.6. Government to consider increased protections for information sharing not currently included in documents such as the ACSC Deed of Confidentiality. These could include protections from liability,

regulation and civil actions, non-waiver of privilege, protection of intellectual property and confidentiality and protections from FOI requests.

3.4.7. Government to establish a national governance framework to ensure consistency and connectivity across the JCSCs and with the ACSC, and to set clear national priorities to deliver programs of work in collaboration with industry.

3.4.8. Government to increase empowerment of JCSCs and strengthen their local leadership.

3.4.9. Industry JCSC Board/Steering Committee members to work with government to review and standardise a tiered engagement model.

3.4.10. Trusted, long-term industry partners in the JCSCs to nominate trusted individuals within threat intelligence companies as a first step towards embedding approved vendors.

3.4.11. Government to establish agreed day(s) for specific industries or practitioner roles to visit the JCSCs – like the Super Drop-In Day in Melbourne, which has been a positive experience.

3.4.12. Government to share advice in advance of announcements and decisions that may impact industry, via the JCSCs (e.g.: attributing high-profile cyber-attacks to foreign governments).

04 Policy Cooperation

4.1. Australian Government use of offensive cyber capabilities

The Australian Government's decision to acknowledge that it possesses offensive cyber capabilities in 2016 was a welcome move. Whilst many in the community are aware of the capabilities housed in the ASD and the Department of Defence, increased transparency around this capability is an important step in signalling internationally that we possess these capabilities. Increased transparency around offensive cyber capabilities (and their use in line with Australian and international law) is also an important step in building trust and confidence and reducing the risk of miscalculation or misunderstanding online.

Australia is also actively working with other governments to effect several norms for appropriate state behaviour online, including the norm that critical infrastructure is 'off-limits' to attack by governments. An official Australian Government definition and list of critical infrastructure sectors would support this work.

4.2. Cyber response exercises

The Government has established a team within the ACSC to deliver cyber security crisis response exercises. A key initiative of the 2016 strategy, this team has carried out valuable work training staff to deliver cyber security exercises within private sector organisations and is developing an energy sector crisis response exercise. Exercises are a key tool to improve coordination between industry and government during a crisis and we believe government should look to build on this program to conduct regular national cross-sector exercises.

4.3. International cooperation

For Telstra, international cooperation with governments and other large telecommunications and technology companies is crucial to help positively shape the security of the global cyber ecosystem. Our heritage is proudly Australian, but we have a longstanding international presence with a focus on the Asia-Pacific region. We operate in 20 countries outside of Australia and hold telecommunications licences in Asia, Europe and the Americas, as well as 2,000 points-of-presence in more than 200 countries and territories globally.

Internationally, Australian advocacy efforts by both government and industry will remain vital in promoting the careful balance between maintaining the rule of law online and ensuring the continued openness and democratisation of the internet. We welcomed the opportunity to contribute to *Australia's International Cyber Engagement Strategy* and the *2019 Progress Report* and acknowledge the leadership role the Department of Foreign Affairs and Trade (DFAT) has taken on the global stage in building capacity and shaping acceptable rules for state behaviour online.

In May 2019, Telstra partnered with DFAT and the ACSC to deliver a session on supply chain risk at the most recent meeting of the Pacific Island Cyber Security Operational Network (PacSON) in Tonga. PacSON is comprised of 15 member governments from the Pacific islands and is designed to facilitate cooperation and build cyber capacity across the region. Representatives included both technical and policy experts from computer emergency response teams (CERTs) and ministerial departments, which allowed for a discussion that canvassed both technical and national security issues.

We are currently working with the World Economic Forum's Centre for Cyber Security and global telecommunications providers on initiatives to counter cyber threats facing the global population. The group is working to establish best practice principles for ISPs on cyber security and protecting customers at scale. Telstra has also become a member of the Global Forum on Cyber Expertise (GFCE), a joint government-industry body established by the Dutch Government for the delivery of joint projects to improve cyber security. The GFCE provides an effective way to tackle 'big cyber problems' that are too costly or complex for organisations to counter alone.

4.4. Recommendations

4.4.1. Government to provide an official, consistent definition as to what is considered 'critical infrastructure' in Australia, to better support policy cooperation with other Governments.

4.4.2. Government to create a central, easily accessible location for the publication of policy positions and documents on the use of offensive cyber capabilities.

4.4.3. Government to develop and lead regular national cross-sector crisis response exercises to test

the national *Cyber Incident Management Arrangements* (CIMA). Specifically, scenarios exploring the *sustained disruption of essential systems and associated services, affecting CNI* and with *potential national security implications* would allow government and industry to establish mutual expectations and thresholds for a nationally-significant cyber crisis event. Running these exercises at a regular cadence e.g. annually, would encourage continuous improvement, build strong partnerships and provide a mechanism for regular measurement of industry-wide cyber maturity.

4.4.4. Where proper and appropriate, government to utilise the expertise that lies within Australian industry when engaging with international counterparts on cyber security issues.

05 Building Enterprise and Skills, Influencing Behavioural Change

5.1. Innovation and the cyber security market

Technology has been making our lives easier, our work more productive and people more connected for many years. What is new is the convergence of several breakthrough technologies. As the connecting platform, 5G will sit at the heart of this revolution. 5G is launching at the same time as other foundational technologies - such as cloud, AI and machine learning, edge compute and software defined networks - are converging and maturing. As we move into the 2020s and the fourth industrial revolution, the combination of these technologies will propel the world forward in automation and robotics, leading to extraordinary economic and productivity gains.

5G is important for several reasons:

- Latency in 5G will eventually be in the single milliseconds
- 5G will have 10 times the capacity of 4G, and a hundred times that of 3G
- 5G is the first telecommunications technology specifically designed to connect things other than mobile phones.

Today we can connect around 10,000 devices in one cell coverage area on a 4G network. On 5G that increases 100-fold to a million. We are seeing an explosion in the number of connected things; it is estimated that by 2023 there will be 50 billion connected things in the world. 5G will enable this growth.

Securing the next generation of our mobile networks is also at the forefront of Telstra's security priorities; whilst the benefits that 5G will bring to the Australian economy are significant, this monumental technological shift will also introduce a complex set of security challenges. The 5G network will serve as the mesh through which our future economy will operate and grow, supported by rapid technological developments in the IoT space. Interconnected devices are gradually permeating throughout our critical infrastructure, particularly in telecommunications, transport and energy. Ensuring we maintain a laser focus on 5G security is of paramount importance. This includes increased attention on supply chain and vendor security. Telstra's robust security practices will ensure that our future economy is built with a secure foundation.

In addition to maintaining 5G security, IoT ecosystem and mass market devices must also be safe and secure. This should involve defining what acceptable hardware and software standards look like. The Internet of Things Alliance Australia's (IoTAA) *Internet of Things Security Guideline* has established a best practice model that provides strategic guidance on the practical application of security to IoT devices, promotes a 'security by design' approach and assists industry to understand some of the relevant legislation around IoT privacy and security. Telstra supports industry and government collaboration in further refining and improving best practice standards such as these as outlined in recommendation (1.4.3.) above.

Beyond 5G and IoT, much of this emerging technology is so new we are yet to fully understand as a society and a nation the benefits and potential security implications they bring. There is an opportunity for industry and government to come together to look 'over the horizon' at emerging technology to identify both the opportunities and risks that will need to be managed as we move into this exciting future. Telstra works to create a protected and resilient environment through driving a shared accountability mindset within our organisation and externally. It is our aim to build security into everything we do, from our core network to our products and services. This forms a strong foundation from which our people can confidently embrace innovation while managing risk.

Some of the ways we are achieving this include:

- Integrating early security engagement into project design and Agile development processes
- A dedicated Secure Code team that works with our developer community to ensure that software is built securely, that source code is handled and stored securely, and that teams follow best practice in their build and deployment pipelines.

We have also created a cohort of 'security champions' within our software development teams, to enable us to scale the support and services they need to deliver and operate secure software solutions at speed. This ongoing training and development program is designed to upskill developer teams to include security throughout the software development lifecycle.

Telstra recognises that the security of Australian homes and small businesses is a major concern for the Government, and we are committed to doing our bit to help, including providing free Domain Name System (DNS) malware protection on all Telstra broadband services.

Providing security solutions at a national scale and affordable price is a capital-intensive endeavour with challenging economics. It entails building in protection 'upstream' at the network rather than device level to reduce consumer risk – a model sometimes referred to as 'clean pipes'. There is a real opportunity for industry and government to work together to design innovative ways to provide safer internet for all, both cost-effectively and at scale. This will require a cross-industry effort to understand our own individual existing protective capabilities and if they are complementary, and for us to explore with government potential commercial models that may deliver even greater protections to the Australian public.

5.2. Skills for the future

Technology will continue to drive changes in our lives and in the workplace – the real issue is how we respond and prepare ourselves for the future. As we look at the future of our business and the work we will be doing, we are confronted with a growing problem. It is one that many other businesses are also facing – demand for highly-skilled technology talent is vastly outstripping supply.

The problem we face as a business is a numbers game: today, we cannot find the skills we need in Australia at the scale we need them. It is estimated Australia will have a shortfall of 60,000 skilled ICT workers in the next five years. For more global context, Australia had around 1,200 new software engineers in the last 12 months, compared to 44,000 in India. That means for every new software engineering graduate in Australia, there are 40 in India. Australia must build more of these skills locally, and as one of the country's biggest employers we are committed to play a part in this.

We are partnering with Australian tertiary institutions to help broaden the talent pipeline for our current and future business needs. One way we are doing this is by establishing a partnership program with five Australian universities to jointly develop the technology skills and capabilities Australia needs for the innovative workplaces of the future.

We have signed Memoranda of Understanding with RMIT University, University of Melbourne, UNSW Sydney, University of Sydney and University of Technology Sydney. Under these agreements, we will work with each university to enhance student learning through placements and work integrated experiences, research and innovation opportunities, and more development including early access to career opportunities.

These memoranda will stay in place for at least two years and we are currently working with our university partners on the first set of priorities under the agreements. Ultimately, we want to develop useful opportunities for students to learn from industry experts and to gain real world experience. We want to help graduates become skilled ICT practitioners who are prepared for the workforce of the future from the moment they are handed their degree.

A diversity of talent

As we look to the future, we will also need to support greater diversity in all its forms. The technology industry is a male-dominated space, and we are committed to ensuring the pipeline of future talent is diverse from its beginning. To do this, our partnerships will look at ways to build curiosity in technology careers and engage a broad range of people before they reach university, including high school student outreach programs.

This early outreach extends to work we are doing through our summer vacation program and our partnership with the Pathways in Technology (P-TECH) program to give more high school students the opportunity to develop an interest and skills in technology.

It also includes acknowledging that we have a depth and breadth of expertise within our organisation and across the industry, and that there are many diverse pathways into a cyber security career. Building the workforce of the future is an urgent challenge. Telstra is determined to be part of the solution.

5.3. From cyber awareness to cyber influence

Technology is widely seen as a critical element of an effective cyber security defence, but less attention is often paid to the human factor. Human error on its own accounts for more than a third of all data breaches reported to the Office of the Australian Information Commissioner (OAIC) since the introduction of the mandatory data breach notification scheme. However, traditional efforts across the industry to address this to date have largely focused on "awareness" – informing individuals of cyber security threats and ways to mitigate them.

What is needed is a shift in mindset: from awareness to influence. Influence (ultimately the desired outcome of an awareness program) requires a deep understanding of your customer; a focus on human behaviour and the needs and wants of your audience.

Security education must be personal, compelling, and relevant. It must be delivered in the mediums your audience consumes information; brochures and fact sheets will not achieve cultural change. It must ultimately motivate the audience to take an action because it is in their interest to do so.

A credible and trusted brand identity is also crucial to effectively influence an audience. Consumers will engage with and act on messages they see to be authentic and dependable; the reputation of the entity delivering the message is just as important as the message itself. This requires an organisation to look inwardly and determine how they may be perceived by their customers or stakeholders. Does the organisation provide unclear, inconsistent, outdated or impractical cyber security advice? Or are they seen as a trusted partner who supports and adds value?

Various government agencies (including the Australian Competition and Consumer Commission, Australian Cyber Security Centre, and Australian Signals Directorate) run individual cyber security awareness campaigns, such as Stay Smart Online Week and Scams Awareness Week, that have contributed to improving community engagement with and understanding of cyber security.

Telstra recognises the important role these campaigns play and is fully supportive of such initiatives. These multiple channels may, however, create a level of confusion within the community on where to go for help. A singular online brand identity for cyber security within government could provide greater clarity; cyber.gov.au is well positioned to be promoted as a central voice of authority for cyber security for the broader public. This would also provide greater opportunities for industry to partner with the government on community-based cyber security initiatives and amplify cyber.gov.au brand and messaging.

Storytelling

Storytelling serves as a foundational component of any influence campaign. Good stories are shared and retold, while mnemonics and slogans (like Telstra's *Five Knows of Cyber Security* or the Australian Cyber Security Centre's *Essential Eight)* help make information memorable.

Millions of Australians and New Zealanders easily recall the 1980s skin cancer awareness program '*Slip, Slop, Slap*' and its message to "slip on a shirt, slop on sunscreen, and slap on a hat", but precious few would recall the numbers of deaths per year from the disease.

Telstra has worked with creative agencies to develop story-driven video content more akin to a Netflix series than a traditional talking-head training video. Staff who viewed our video miniseries shared it with friends, family, and colleagues in an amplification of our security message – not by a request to do so, but because the content is engaging and relatable.

5.4. Recommendations

5.4.1. Government to use levers such as tax, immigration and business policies that incentivise investment, research and innovation to create a legislative and economic environment that supports growth in the cyber security talent pipeline and supply chain.

5.4.2. Government and key industry partners such as Telstra to jointly map internal cyber security technical capabilities to categorise where existing capabilities lie across industry and government, how they could potentially be cross-utilised, and where skills gaps exist that need to be developed or sourced.

5.4.3. Government to develop an accreditation scheme for cyber security higher education courses that is tied to the US National Initiative for Cybersecurity Education (NICE) framework to ensure shared

expectations of the skills taught in these courses and the job opportunities that match their qualifications.

5.4.4. Government to promote a central, singular online brand identity (such as cyber.gov.au) for government cyber security messaging that delivers ongoing, engaging education initiatives in partnership with industry.

5.4.5. Industry and government to come together to perform a 'horizon-scan' of emerging technologies to identify both the opportunities and risks they present. This should look to leverage whole-of-government expertise and industry knowledge and seek to identify potential strategic security issues.

5.4.6. Cross-industry study involving major ISPs to understand existing 'clean-pipes' initiatives and an exploration with government around potential commercial models that may deliver even greater upstream network protections to the Australian public.

06 Appendix

6.1. Map of discussion paper questions to Telstra recommendations

Discussion paper questions	Telstra recommendations	Status (ongoing from 2016 strategy or new initiative)
1. What is your view of the cyber threat environment? What threats should Government be focusing on?	1.4.1 Industry and government to form an expert group to agree priority network-level threats and together engage the most appropriate global forums for the promotion and adoption of security best practice to address these (e.g.: Mutually Agreed Norms for Routing Security (MANRS) for BGP). 1.4.2 Industry and government to form Australian Cyber Security Centre (ACSC)-led cross-sector working groups to consolidate visibility of high-volume cybercrime impacting consumers, and identify existing capabilities, processes and legislative tools to address this threat. 1.4.4 Industry and government to form joint threat intelligence cells which co-locate practitioners within the JCSCs and/or ACSC, to focus on monitoring and countering new actors and techniques that are high-effort and high-impact 2.5.1 Government to undertake an annual national stocktake to quantify the scale and cost of cyber threats to Australia, share these insights publicly and use them to inspire evidence-based conclusions as to which	1.4.1 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy. 1.4.2 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy. 1.4.4. This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 2.5.1 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy.

	programs may be making an impact to improve national resilience.	
2. Do you agree with our understanding of who is responsible for managing cyber risks in the economy? 3. Do you think the way these responsibilities are currently allocated is right? What changes should we consider?	4.4.2 Government to create a central, easily accessible location for the publication of policy positions and documents on the use of offensive cyber capabilities. 4.4.4 Where proper and appropriate, government to utilise the expertise that lies within Australian industry when engaging with overseas counterparts on cyber security issues. 2.5.5 Government and industry to consult on advanced threats to develop a risk- and threat-based collaborative response model	4.4.2 This is a new recommendation. 4.4.4 This is a new recommendation. 2.5.5 This is a new recommendation.
4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?	1.4.1 Industry and government to form an expert group to agree priority network-level threats and together engage the most appropriate global forums for the promotion and adoption of security best practice to address these (e.g.: Mutually Agreed Norms for Routing Security (MANRS) for BGP). 1.4.2 Industry and government to form Australian Cyber Security Centre (ACSC)-led cross-sector working groups to consolidate visibility of high-volume cybercrime impacting consumers, and identify existing capabilities, processes and legislative tools to address this threat. 1.4.4 Industry and government to form joint threat intelligence cells which co-locate practitioners within the JCSCs and/or ACSC, to focus on monitoring and countering new actors and techniques that are high-effort and high-impact 2.5.1 Government to undertake an annual national stocktake to	1.4.1 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy. 1.4.2 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy. 1.4.4 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 2.5.1 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy. 2.5.2 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 2.5.4 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy. 2.5.5 This is a new recommendation.

	quantify the scale and cost of cyber threats to Australia, share these insights publicly and use them to inspire evidence-based conclusions as to which programs may be making an impact to improve national resilience. 2.5.2 Industry to repeat the ASX100 cyber health check, improving on previous surveys by undertaking a split model approach and clarifying definitions of terms used. 2.5.4 Government to re-establish previous regular quarterly operational meetings between the Minister responsible for cyber security and key industry CISOs. These meetings provided Ministers with front-line insights on key cyber security issues and opportunities for greater collaboration. Representation should cover key sectors including telecommunications, financial services, energy, healthcare, education and resources. 2.5.5 Government and industry to consult on advanced threats to develop a risk- and threat-based collaborative response model 3.4.2 Government to appoint a dedicated, visible, senior ACSC leader to be given responsibility for two-way engagement with CNI organisations on sensitive cyber security threats. This position would replace the current arrangements that often see industry advised to send sensitive information to a generic ACSC mailbox. 3.4.7 Government to establish a national governance framework to ensure consistency and connectivity across the JCSCs and with the ACSC, and to set clear national priorities to deliver programs of work in collaboration with industry.	3.4.2 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.7 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.12 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy.

	3.4.12 Government to share advice in advance of announcements and decisions that may impact industry, via the JCSCs, (e.g.: attributing high-profile cyber-attacks to foreign governments).	
5. How can Government maintain trust from the Australian community when using its cyber security capabilities?	5.4.4 Government to promote a central, singular brand identity (such as cyber.gov.au) for government cyber security messaging that delivers ongoing, engaging education initiatives, in partnership with industry.	5.4.4 This recommendation builds on "Global Responsibility and Influence" action items in the 2016 cyber security strategy.
6. What customer protections should apply to the security of cyber goods and services?	1.4.3 Industry to lead the development of best practice software standards to reduce impacts of potential attacks via mass market devices (e.g.: home automation, security cameras, drones, etc) leveraging existing standards such as the Internet of Things Alliance Australia's (IoTAA) *Internet of Things Security Guideline.* Government to endorse standards where appropriate to support wider adoption.	1.4.3 This is a new recommendation.
7. What role can Government and industry play in supporting the cyber security of consumers?	1.4.3 Industry to lead the development of best practice software standards to reduce impacts of potential attacks via mass market devices (e.g.: home automation, security cameras, drones, etc) leveraging existing standards such as the Internet of Things Alliance Australia's (IoTAA) *Internet of Things Security Guideline.* Government to endorse standards where appropriate to support wider adoption. 2.5.4 Government to re-establish previous regular quarterly operational meetings between the Minister responsible for cyber security and key industry CISOs. These meetings provided Ministers with front-line insights on key cyber security issues and opportunities for greater collaboration. Representation should cover key sectors including telecommunications,	1.4.3 This is a new recommendation. 2.5.4 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy. 2.5.6 This is a new recommendation. 5.4.6 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy.

	financial services, energy, healthcare, education and resources. 2.5.6 To ensure regulation is effective, Government to pursue consistency of obligations across providers of same services, whether or not traditionally licensed. 5.4.6 Cross-industry study involving major ISPs to understand existing 'clean-pipes' initiatives and an exploration with government around potential commercial models that may deliver even greater upstream network protections to the Australian public.	
8. How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?	1.4.2 Industry and government to form Australian Cyber Security Centre (ACSC)-led cross-sector working groups to consolidate visibility of high-volume cybercrime impacting consumers, and identify existing capabilities, processes and legislative tools to address this threat. 1.4.3 Industry to lead the development of best practice software standards to reduce impacts of potential attacks via mass market devices (e.g.: home automation, security cameras, drones, etc) leveraging existing standards such as the Internet of Things Alliance Australia's (IoTAA) *Internet of Things Security Guideline.* Government to endorse standards where appropriate to support wider adoption. 5.4.5 Industry and government to come together to perform a 'horizon-scan' of emerging technology to identify both the opportunities and risks they present. This should look to leverage whole-of-government expertise and industry knowledge and seek to identify potential strategic security issues.	1.4.2 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy. 1.4.3 This is a new recommendation. 5.4.5 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy.
9. Are there functions the Government currently performs		

that could be safely devolved to the private sector? What would the effect(s) be?		
10. Is the regulatory environment for cyber security appropriate? Why or why not? 11. What specific market incentives or regulatory changes should Government consider?	2.5.1 Government to undertake an annual national stocktake to quantify the scale and cost of cyber threats to Australia, share these insights publicly and use them to inspire evidence-based conclusions as to which programs may be making an impact to improve national resilience. 2.5.4 Government to re-establish previous regular quarterly operational meetings between the Minister responsible for cyber security and key industry CISOs. These meetings provided Ministers with front-line insights on key cyber security issues and opportunities for greater collaboration. Representation should cover key sectors including telecommunications, financial services, energy, healthcare, education and resources. 2.5.5 Government and industry to consult on advanced threats to develop a risk- and threat-based collaborative response model 2.5.6 To ensure regulation is effective, Government to pursue consistency of obligations across providers of same services, whether or not traditionally licensed. 3.4.3 Government to extend existing Slack groups to include industry verticals and/or thematic streams curated by ACSC sector/theme leads (e.g.: Open Source Intelligence, telco). These lead analysts promote discussion and collaboration and disseminate relevant, actionable information to the group. 3.4.5 Industry and Government to further enable cross-industry sharing by conducting an assessment on potential legislative barriers to sharing	2.5.1 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy. 2.5.4 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy. 2.5.5 This is a new recommendation. 2.5.6 This is a new recommendation. 3.4.3 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.5 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.7 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.10 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.11 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.12 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 4.4.1 This is a new recommendation. 4.4.2 This is a new recommendation. 4.4.3 This recommendation builds on "Strong Cyber Defences"

	anonymised information e.g.: privacy legislation and work with industry on solutions. 3.4.7 Government to establish a national governance framework to ensure consistency and connectivity across the JCSCs and with the ACSC, and to set clear national priorities to deliver programs of work in collaboration with industry. 3.4.10 Trusted, long-term industry partners in the JCSCs to nominate trusted individuals within threat intelligence companies as a first step towards embedding approved vendors. 3.4.11 Government to establish agreed day(s) for specific industries or practitioner roles to visit the JCSCs – like the Super Drop-In Day in Melbourne, which has been a positive experience. 3.4.12 Government to share advice in advance of announcements and decisions that may impact industry, via the JCSCs, (e.g.: attributing high-profile cyber-attacks to foreign governments). 4.4.1 Government to provide an official, consistent definition as to what is considered 'critical infrastructure' in Australia, to better support policy cooperation with other Governments. 4.4.2 Government to create a central, easily accessible location for the publication of policy positions and documents on the use of offensive cyber capabilities. 4.4.3 Government to develop and lead regular national cross-sector crisis response exercises to test the national *Cyber Incident Management Arrangements (CIMA).* Specifically, scenarios exploring the *sustained disruption of essential systems and associated services, affecting CNI* and with *potential national security implications* would allow government and industry to establish mutual expectations and thresholds for a nationally-	action items in the 2016 cyber security strategy.

	significant cyber crisis event. Running these exercises at a regular cadence e.g. annually, would encourage continuous improvement, build strong partnerships and provide a mechanism for regular measurement of industry-wide cyber maturity.	
12. What needs to be done so that cyber security is 'built in' to digital goods and services?	1.4.3 Industry to lead the development of best practice software standards to reduce impacts of potential attacks via mass market devices (e.g.: home automation, security cameras, drones, etc) leveraging existing standards such as the Internet of Things Alliance Australia's (IoTAA) *Internet of Things Security Guideline.* Government to endorse standards where appropriate to support wider adoption.	1.4.3 This is a new recommendation.
13. How could we approach instilling better trust in ICT supply chains?		
14. How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?	5.4.1 Government to use levers such as tax, immigration and business policies that incentivise investment, research and innovation to create a legislative and economic environment that supports growth in the cyber security talent pipeline and supply chain. 5.4.2 Government and key industry partners such as Telstra to jointly map internal cyber security technical capabilities to categorise where existing capabilities lie across industry and government, how they could potentially be cross-utilised, and where skills gaps exist that need to be developed or sourced. 5.4.3 Government to develop an accreditation scheme for cyber security higher education courses that is tied to the US National Initiative for Cybersecurity Education (NICE) framework to ensure shared expectations of the skills taught in these courses	5.4.1 This recommendation builds on "A Cyber Smart Nation" action items in the 2016 cyber security strategy. 5.4.2 This recommendation builds on "A Cyber Smart Nation" action items in the 2016 cyber security strategy. 5.4.3 This recommendation builds on "A Cyber Smart Nation" action items in the 2016 cyber security strategy.

	and the job opportunities that match their qualifications.	
15. Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?		
16. How can high-volume, low-sophistication malicious activity targeting Australia be reduced? 17. What changes can Government make to create a hostile environment for malicious cyber actors?	1.4.2 Industry and government to form Australian Cyber Security Centre (ACSC)-led cross-sector working groups to consolidate visibility of high-volume cybercrime impacting consumers, and identify existing capabilities, processes and legislative tools to address this threat. 1.4.3 Industry to lead the development of best practice software standards to reduce impacts of potential attacks via mass market devices (e.g.: home automation, security cameras, drones, etc) leveraging existing standards such as the Internet of Things Alliance Australia's (IoTAA) *Internet of Things Security Guideline.* Government to endorse standards where appropriate to support wider adoption. 2.5.1 Government to undertake an annual national stocktake to quantify the scale and cost of cyber threats to Australia, share these insights publicly and use them to inspire evidence-based conclusions as to which programs may be making an impact to improve national resilience.	1.4.2 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy. 1.4.3 This is a new recommendation. 2.5.1 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy.
18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?	2.5.4 Government to re-establish previous regular quarterly operational meetings between the Minister responsible for cyber security and key industry CISOs. These meetings provided Ministers with front-line insights on key cyber security issues and opportunities for greater collaboration. Representation should cover key sectors including telecommunications, financial services, energy,	2.54 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy. 4.4.3 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy.

	healthcare, education and resources. 4.4.3 Government to develop and lead regular national cross-sector crisis response exercises to test the national *Cyber Incident Management Arrangements (CIMA).* Specifically, scenarios exploring the *sustained disruption of essential systems and associated services, affecting CNI* and with *potential national security implications* would allow government and industry to establish mutual expectations and thresholds for a nationally-significant cyber crisis event. Running these exercises at a regular cadence e.g. annually, would encourage continuous improvement, build strong partnerships and provide a mechanism for regular measurement of industry-wide cyber maturity.	
19. What private networks should be considered critical systems that need stronger cyber defences?	4.4.1 Government to provide an official, consistent definition as to what is considered 'critical infrastructure' in Australia, to better support policy cooperation with other Governments.	4.4.1 This is a new recommendation.
20. What funding models should Government explore for any additional protections provided to the community?	5.4.6 Cross-industry study involving major ISPs to understand existing 'clean-pipes' initiatives and an exploration with government around potential commercial models that may deliver even greater upstream network protections to the Australian public.	5.4.6 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy.
21. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?	3.4.1 Industry to nominate issues of interest for discussion in advance of information exchange meetings (i.e.: country or vector) so that relevant Canberra-based experts can attend and provide more in-depth insights from a government perspective. 3.4.2 Government to appoint a dedicated, visible, senior ACSC leader to be given responsibility for two-way engagement with	3.4.1 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.2 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.3 This recommendation builds on "Strong Cyber Defences"

	CNI organisations on sensitive cyber security threats. This position would replace the current arrangements that often see industry advised to send sensitive information to a generic ACSC mailbox. 3.4.3 Government to extend existing Slack groups to include industry verticals and/or thematic streams curated by ACSC sector/theme leads (e.g.: Open Source Intelligence, telco). These lead analysts promote discussion and collaboration and disseminate relevant, actionable information to the group. 3.4.4 Government to lower the classification of information where possible and create more actionable advice for small businesses reflective to the size and capability of the organisations represented. 3.4.5 Industry and Government to further enable cross-industry sharing by conducting an assessment on potential legislative barriers to sharing anonymised information e.g.: privacy legislation and work with industry on solutions. 3.4.6 Government to consider increased protections for information sharing not currently included in documents such as the ACSC Deed of Confidentiality. These could include protections from liability, regulation and civil actions, non-waiver of privilege, protection of intellectual property and confidentiality and protections from FOI requests. 3.4.7 Government to establish a national governance framework to ensure consistency and connectivity across the JCSCs and with the ACSC, and to set clear national priorities to deliver programs of work in collaboration with industry.	action items in the 2016 cyber security strategy. 3.4.4 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.5 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.6 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.7 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.8 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.9 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.10 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy. 3.4.11 This recommendation builds on "Strong Cyber Defences" action items in the 2016 cyber security strategy.

	3.4.8 Government to increase empowerment of JCSCs and strengthen their local leadership. 3.4.9 Industry JCSC Board/Steering Committee members to work with government to review and standardise a tiered engagement model. 3.4.10 Trusted, long-term industry partners in the JCSCs to nominate trusted individuals within threat intelligence companies as a first step towards embedding approved vendors. 3.4.11 Government to establish agreed day(s) for specific industries or practitioner roles to visit the JCSCs – like the Super Drop-In Day in Melbourne, which has been a positive experience.	
22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings? 23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products? 24. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?	5.4.4 Government to promote a central, singular brand identity (such as cyber.gov.au) for government cyber security messaging that delivers ongoing, engaging education initiatives, in partnership with industry.	5.4.4 This recommendation builds on "Global Responsibility and Influence" action items in the 2016 cyber security strategy.
25. Would you like to see cyber security features prioritised in products and services?	2.5.7 Government to explore ways to adjust policy settings to help address technology challenges introduced by interdependencies with OTT providers.	2.5.7 This is a new recommendation.
26. Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?	2.5.3 Government to establish a 2020 Cyber Security Strategy CEO industry advisory panel to provide input, advice and guidance on the ongoing implementation of the 2020 strategy initiatives.	2.5.3 This recommendation builds on "A National Cyber Partnership" action items in the 2016 cyber security strategy.