South Australian Government

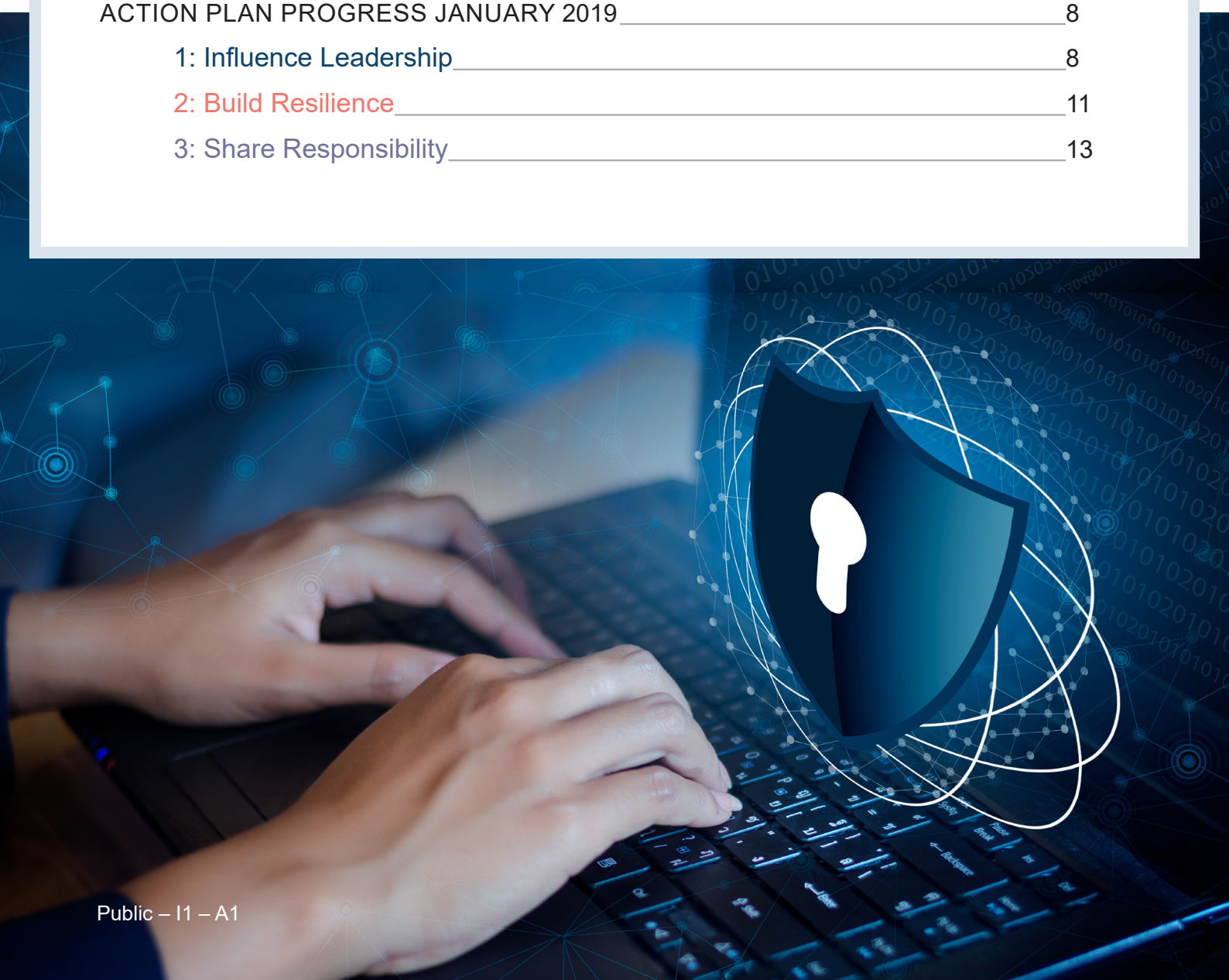
CYBER SECURITY STRATEGIC PLAN 2018-2021

Progress Report January 2019

Government of South Australia

SOUTH AUSTRALIA

CONTENTS



FOREWORD

South Australia has held a status as one of the leading jurisdictions for cyber security due to major initiatives such as:

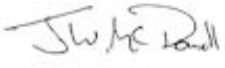
- A whole of government cyber security policy (the Information Security Management Framework) aligned to international standards.
- One of the country's largest centralised government network (StateNet) and mail system which provide significant security measures whilst achieving economies of scale.
- A cyber security intelligence function that works with police, emergency services and national security organisations to monitor and respond to major incidents.
- Having 'cyber crisis' as a recognised incident type in the South Australian security and emergency management legislative arrangements.
- A "Top Ten Cyber Resilience and Preparedness Objectives" program which measures all agency's maturity against 10 key cyber security objectives.

The ability for the government and South Australia to deliver on a digital and innovation agenda and truly gain the benefits of innovative industries such as space and defence relies on trust and confidence.

Robust cyber security is essential for maintaining the confidence and trust of customers. It is essential for maintaining the wide array of services provided by the government, including those essential to community safety and well-being such as health, emergency services, energy, water or transport.

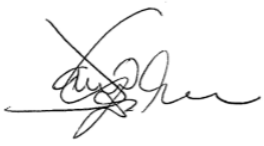
The South Australian Cyber Security Strategic Plan and the delivery of the activities will strengthen our cyber security capability and maturity and reflects the State Government's commitment to ensuring that South Australia is a safe, secure and resilient place to live and for business for all South Australians.

Endorsed by



Mr Jim McDowell
Chief Executive,
Department of the Premier and Cabinet
Government of South Australia

Mr Rick Persse
Chair, ICT and Digital Board
Chief Executive,
Department for Education
Government of South Australia



Mr David Goodman
Chief Information Security Officer
Government of South Australia

EXECUTIVE SUMMARY

The South Australian Government Cyber Security Strategic Plan 2018 – 2021 was released in February 2018.

The strategic plan sets out the following three strategic themes.

Influence Leadership

Through leadership of the Office for Cyber Security, we will strengthen the role of government in providing sound governance and clear accountabilities for a whole of government approach to cyber security.

Build Resilience

We will strengthen the approach to the prevention of, detection of, response to and recovery from cyber security threats and incidents.

Share Responsibility

We will cultivate a collaborative approach that brings together all levels of government with academia and the private sector to cyber security.

Attached to each of these three themes are several strategic objectives. A program of 39 key activities formed the 'Action Plan' for the period 2018 to 2021.

Since the release, significant work has been undertaken across the three strategic themes that have been instrumental in providing the South Australian Government with a stronger cyber security direction and foundation for future deliverables.

Our vision "Protecting the Present – Enabling the Future" is reflected in the activities within the strategic plan.

To ensure that the strategic plan remains relevant and continues delivering the outcomes on time, a review has been undertaken. More details about the progress of all activities can be found in the Section, 'Action Plan Progress January 2019'.

DELIVERING THE STRATEGY

Some notable achievements from the strategic plan during 2018 are:

01 South Australian Government Cyber Security Strategic Plan 2018 – 2021 was released in February 2018.

02 StateNet Conditions of Connection was updated and issued.

03 An across South Australian Government Cyber Security Steering Committee has been established.

04 The across South Australian Government IT Security Advisor [ITSA] Forum has been re-established with regular ITSA forums being held throughout 2018.

05 The Office for Cyber Security has increased participation and an active role on behalf of the South Australian Government in membership of relevant boards, committees and bodies in SA, nationally, and internationally to influence national cyber security initiatives.

06 An independent Cyber Security Resilience review on South Australian Government agenices was completed.

07 A Cyber Terrorism exercise (funded by Australia-New Zealand Counter Terrorism Committee) was undertaken.

08 In conjunction with CERT Australia, the Office for Cyber Security delivered cyber security exercises for SEMC, DPC Control Agency for ICT Failure, and agency ITSAs.

09 Cyber Insurance arrangements through the South Australian Government captive insurer (SAicorp) were reviewed.

10 A Cyber Threat Intelligence Sharing Toolkit was deployed to South Australian Government agencies.

11 The Office for Cyber Security Watch Desk facility was reviewed and further developed as a respected and leading incident detection, response and advisory group for across government.

12 The Adelaide Joint Cyber Security Centre (JCSC) was opened.

13 The AustCyber SA Node was established, and this is co-located within the JCSC. The JCSC and AustCyber Node programs are key to strengthening and enhancing South Australia's cyber resilience and delivering growth and innovation in cyber security through the collaboration of resources.

14 A review was undertaken on the options available for a State Cyber Security Operations Centre for South Australian Government. The findings and recommendations of this review are being considered for implementation during 2019.

15 Cyber Security Traineeships – Training and Skills Commission approved the TAFE Certificate 4 in Cyber Security as a new traineeship to support the activity SR2.4.

16 Cyber Security Strategic Plan Review Completed.

17 Cyber Security Incidents are included on the 'Emergencies and Safety page of SA.GOV.AU - https://www.sa.gov.au/topics/emergencies-and-safety/cyber-security

BUILDING ON THE STRATEGY

In reviewing the strategy and the outcomes achieved during 2018, it is acknowledged that there are several critical pillars that support the strategic themes. It is important that these are recognised and that future activities identified for implementation will build the maturity in these areas, so that the South Australian Government continues to strengthen its cyber resilience.

Cyber Pillars

Government

Protect all South Australian Government systems and the data held in them to ensure they are secure.

Critical Infrastructure

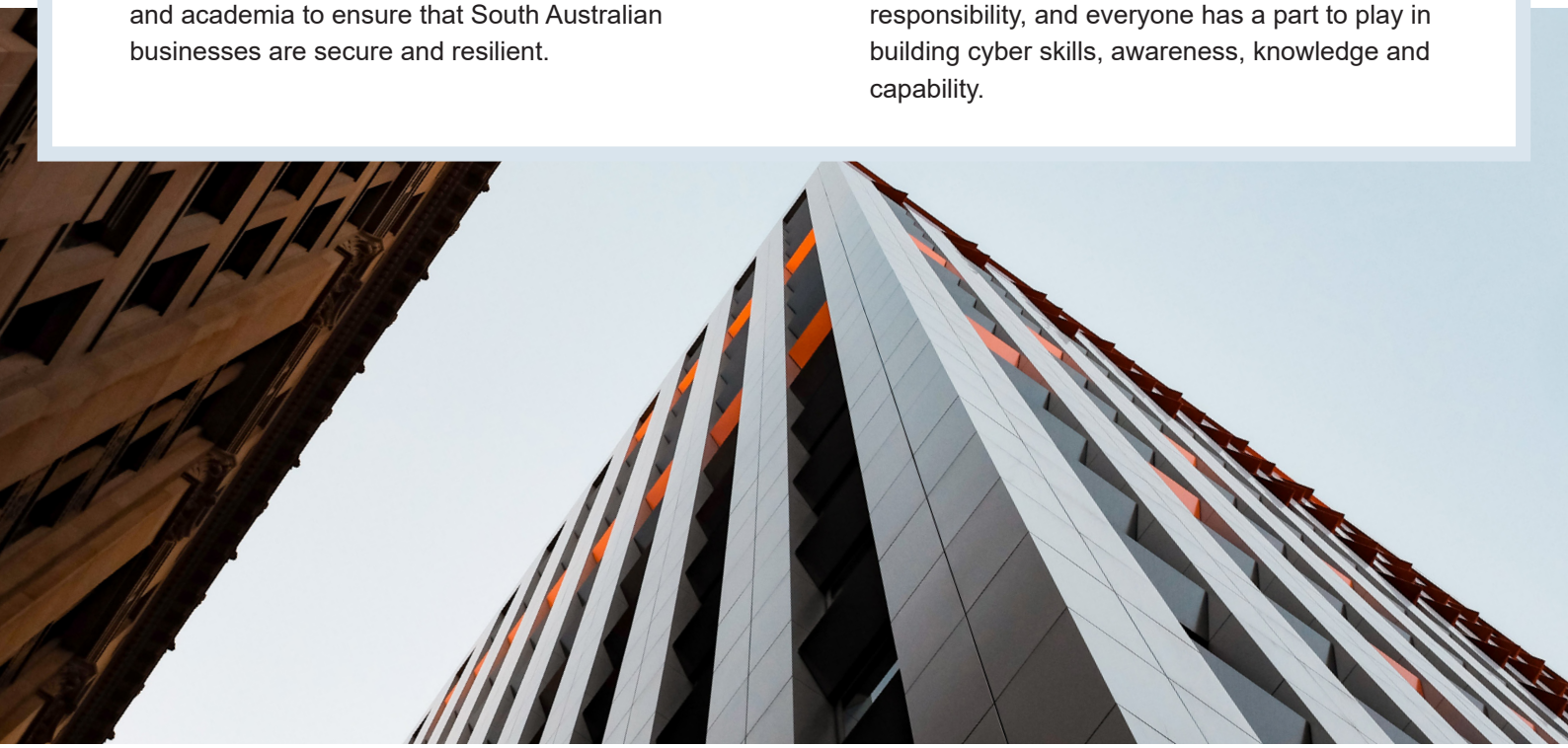
Strengthen the South Australian Government's critical infrastructure cyber resilience.

Business

Work in collaboration with the private sector and academia to ensure that South Australian businesses are secure and resilient.

Citizens

Cyber Security and resilience is a shared responsibility, and everyone has a part to play in building cyber skills, awareness, knowledge and capability.



The South Australian Government, through the Office for Cyber Security, will lead areas of work across government agencies focusing on:

- securing critical infrastructure
- supporting the defence industry supply chain
- building cyber resilience
- accelerating the implementation of Cyber Security traineeships and apprenticeships in South Australia.

NEXT STEPS

The South Australian Government regards the states cyber security resilience as a top priority. Through the Cyber Security Strategic Plan, with strong leadership and governance, the Office for Cyber Security will continue to drive the progress of the initiatives. This will strengthen the cyber security capability and maturity of South Australia, ensuring that it is a safe, secure and resilient place to live, work and visit.

The 'Action Plan Progress January 2019' details the initiatives from the first release of the Cyber Security Strategic Plan 2018 – 2021 which have been completed, are yet to be completed and those which are ongoing. New initiatives, that have been identified as priorities for the next two years, have also been added to the plan.

ACTION PLAN PROGRESS JANUARY 2019

#	Activity	Success Criteria	Progress	Due
Influence Leadership (IL) *Strengthen the role of government in providing sound governance and clear accountabilities for a whole of government approach to cyber security.*				
IL1 - Plan and develop policy frameworks				
1.1	Develop a South Australian Government Cyber Security Strategic Plan.	An approved and published South Australian Government Cyber Security Strategic Plan on SA.GOV.AU by January 2018.	✓	Completed January 2018
1.2	Review the appropriateness and currency of existing cyber security policies for the South Australian Government.	Information Security Management Framework (ISMF) 3.2 to be replaced by a simplified ISMF 4.0, and all associated standards and guidelines reviewed and updated by 30 June 2018.	⏱	June 2019
		Deliver Cloud Security standards and guidelines by 30 June 2018.	⏱	June 2019
		Contribute to the delivery of an updated PC030 – Protective Security Management Framework by June 2018.	⏱	June 2019
		Deliver an updated StateNet Conditions of Connection 4.0 by June 2018.	✓	Completed January 2018
1.3	Implement a continuous improvement program and report regularly to the Senior Management Council on cyber security progress.	Six monthly updates provided to Senior Management Council.	↻	Completed January 2019
		Strategic Plan reassessed and modified in January 2019.	✓	
		*Regular reporting provided to Emergency Management Council. (**NEW**)*	↻	
IL2 - Lead people and change to improve the culture of cyber security				
2.1	Deliver employee training and build awareness about information security.	An across government cyber and information security employee training and awareness package designed.	⏱	June 2019
2.2	Integrate cyber risks within enterprise risk management processes.	Cyber and information security risks are included on operational and corporate risk registers and treated as enterprise level risks.	↻	

⏱ Delayed 📈 Strong Progress ↻ Ongoing ✓ Completed

#	Activity	Success Criteria	Progress	Due
2.3	Encourage trust and confidence in online and digital service delivery.	A reduced number and impact of security incidents related to online and digital delivery of services by January 2019. Full mandatory integration of security considerations in design and implementation of online services.		June 2019
2.4	Support government agencies to ensure employees in positions of trust are appropriately trained and vetted.	Policy for all SA Government staff employed in positions of trust or working in areas delivering critical services to the state by August 2018. Mandatory personal vetting and security screening implemented at a level appropriate to role prior to employment by August 2018. Mandatory security training for staff employed in positions of trust by August 2018.		December 2019
IL3 - Assign government responsibility				
3.1	Establish an across government Cyber Security Governance Committee.	An across government Cyber Security Advisory Sub Committee of the ICT and Digital Governance Board established by January 2018.		Completed January 2018
3.2	Re-establish the across government IT Security Adviser Forum.	Regular ITSA Forums delivered, with improvements to the structure and delivery based on industry and participant feedback by January 2018.		Completed January 2018
3.3	Develop a cyber security profession career path for SA Government.	Defined role guidance for across government security personnel designed by March 2018. An across government mentoring and secondment program established by June 2018. Partnerships with industry and academia established to deliver relevant and suitable training for cyber and information security.		December 2019
3.4	Take an active role in leading and influencing national cyber security initiatives.	Increased participation by the South Australian Government in membership of relevant boards, committees and bodies in SA, nationally, and internationally. Support the Joint Cyber Security Centre program and launch of the centre. Support the Cyber Security Growth Network initiative and launch of the SA node (refer to SR2.1).		Completed November 2018

 Delayed
 Strong Progress
 Ongoing
 Completed

#	Activity	Success Criteria	Progress	Due
3.5 ***NEW***	*Establish an across government Agency Security Executive [ASE] Forum.*	*ASE forums held to assist agency ASE's in delivering their responsibilities under this role.*		March 2019
IL4 - Measure cyber security performance				
4.1	Create a Balance Scorecard for security outcomes.	Independent across government cyber security assessment undertaken by February 2018. Baselines for cyber security metrics set by February 2018. Desired state for Cyber Security maturity defined for government agencies by June 2018.	  	Completed November 2018 June 2019 June 2019
4.2	Support a risk-based prioritisation of government expenditure on cyber security.	Current levels and patterns of expenditure in cyber security across SA Government assessed. Use of economies of scale through across government procurement of cyber services increased.		April 2019
4.3 ***NEW***	*Establish Agency Cyber Security budgeting.*	*Agency budgeting methodology for funding Cyber Security initiatives reviewed with guidance provided to agencies to support procurement of cyber security services and capabilities.*		April 2019
4.4 ***NEW***	*Define the desired state for Cyber Security maturity in government agencies.*	*An across government maturity level is set as a benchmark for all SA Government agencies, aligning to the Top 10 Cyber Resilience and Preparedness Objective Maturity Model. (refer to BR 1.2)*		June 2019
4.5 ***NEW***	*Integrate cyber risk into agency risk framework.*	*A Cyber risk appetite model is developed and agreed, and each agency agree their own risk appetite statement for cyber security.*		December 2019

 Delayed
 Strong Progress
 Ongoing
 Completed

#	Activity	Success Criteria	Progress	Due
Build Resilience (BR) *Strengthen the approach to the prevention of, detection of, response to and recovery from cyber security threats and incidents.*				
BR1 - Prevent and prepare				
1.1	Continue to develop the SA Government's cyber resilience position.	Independent Cyber Resilience Review undertaken by February 2018 (refer to IL4.1). Participation in Australian Government Cyber Resilience activities to ensure alignment with state and national activities.	 	Completed November 2018
1.2	Deliver the ongoing SA Government Top Ten Cyber Resilience and Preparedness Objectives work program.	Top 10 Cyber Resilience and Preparedness Objectives Maturity Model reviewed and evaluated to move from a compliance model to a prescriptive roadmap and planning model and updated in line with revised ISMF.		June 2019
1.3	Develop a whole of government approach for the management of contractual cyber security risks.	Whole of government approach developed, including standard contract clauses by June 2018.		June 2019
1.4	Develop an external/internal vulnerability scanning and assessment capability.	Full program implementation and business process established by January 2020.		January 2020
1.5	Consciously consider emerging cyber threats in the development of intelligence products.	Watch Desk continues to develop its holistic threat intelligence capability. Watch Desk provides timely and accurate cyber threat and intelligence information with regular feedback sought from stakeholders. Delivery of the threat intelligence sharing platforms (refer to SR1.1).		
1.6	Improve security and policy control measures for areas of high risk, including critical infrastructure.	Current security and policy control measures for high risk systems re-examined, with implementation of improvement measures commencing. State Government Critical ICT Infrastructure program redeveloped.		
1.7	Develop a cyber security 'Marketplace' or 'Kiosk'.	Economies of scale achieved through across government procurement of essential cyber security tools/services by July 2018.		December 2019

 Delayed
 Strong Progress
 Ongoing
 Completed

#	Activity	Success Criteria	Progress	Due
1.8	Undertake regular cyber crisis planning, preparedness and response exercises with government and industry partners.	An annual training program delivered each year. Cyber Terrorism exercise (funded by Australia-New Zealand Counter Terrorism Committee) undertaken.	 	Completed June 2018
BR2 - Respond and recover				
2.1	Enhance cyber security incident and crisis management arrangements to improve alignment with Commonwealth, State Crisis and Emergency Management arrangements.	DPC in conjunction with CERT Australia undertake cyber security exercises for SEMC, DPC Control Agency for ICT Failure, and agency ITSAs by January 2018. SA Government response arrangements aligned with the Australian Government cyber crisis management arrangements by June 2018. *Establishment of Telecoms Sector Governance Forum to support emergency response capability. (**NEW**)*	 	Completed January 2018
2.2	Review cyber insurance arrangements for government.	Cyber Insurance arrangements reviewed by June 2018.		Completed March 2018
2.3	Create systems and processes for resource pooling for significant cyber security incident responses.	Implementation of cyber security resources for the management of significant cyber security incident responses by May 2018, taking into account all skillsets required (i.e. more than just cyber security experts). SA Communications Sector Forum's capability and capacity developed through awareness raising exercises by May 2018.		June 2019
BR3 - Grow				
3.1	Document and share lessons learned from significant cyber security incidents to promote cross-sector collaboration.	Formal collaboration tools used by security community for inter-agency sharing of lessons are reviewed and agencies increase their utilisation by December 2018.		
3.2	Establish uniformity of cyber security resourcing across the public sector to ensure adequate resourcing.	Cyber Security Workforce Framework developed by December 2018.		June 2019

 Delayed
 Strong Progress
 Ongoing
 Completed

#	Activity	Success Criteria	Progress	Due
Share Responsibility (SR) *Cultivate a collaborative approach that brings together all levels of government with academia and the private sector to cyber security.*				
SR1 - Share knowledge and threat intelligence				
1.1	Deploy a Threat Intelligence Platform for use by all government agencies.	Cyber Threat Intelligence Sharing Toolkit deployed for agency use by January 2018. Toolkit deployed for private sector partners by June 2018.	 	Completed January 2018 March 2019
1.2	Continue to develop the Watch Desk facility as a respected and leading incident detection, response and advisory group for across government.	Watch Desk facility reviewed, and improvement plan implemented by June 2018.		Completed June 2018
SR2 - Develop partnerships				
2.1	Support the establishment of the SA Node of AustCyber.	SA Node established by January 2018.		Completed November 2018
2.2	Support the establishment of the Joint Cyber Security Centre in Adelaide by the Australian Government.	Joint Cyber Security Centre established and operating in SA by March 2018 with support from SA Government personnel.		Completed November 2018
2.3	Establish strong and improved engagement programs and partnerships with industry.	Partnerships and engagement programs established and continuously improved to achieve optimal outcomes for stakeholders. Ongoing support for the work of the Australian Government Critical Infrastructure Centre. Ongoing support for the Trusted Information Sharing Network model, including participation in appropriate governance groups and involvement in exercises and training.		
2.4	Establish partnerships with academia to ensure suitable education and training is available within SA for cyber security skills growth.	Partnerships and engagement programs established and continuously improved to achieve optimal outcomes for stakeholders. Examine support for the Cyber Security Cooperative Research Centre, with potential opportunities identified by June 2018.		June 2019

 Delayed
 Strong Progress
 Ongoing
 Completed

#	Activity	Success Criteria	Progress	Due
2.5 ***NEW***	*Strengthen and enhance cyber security resilience of South Australia through improved engagement programs and collaboration of resources.*	*Growth and innovation in cyber security with industries delivered through involvement with industry bodies and other government initiatives such as the Adelaide Joint Cyber Security Centre (JCSC), Lot 14, Defence SA, AustCyber and Regional Council of Bretagne.* *Integrating with ACSC/JCSC national collaboration and threat sharing tools.*		December 2019
2.6 ***NEW***	*Support the growth of the South Australian cyber security industry.*	*AustCyber SA Node supported to deliver the activities within South Australia.*		December 2019
SR3 - Build capability				
3.1	Ensure an agile future resource capability by providing appropriate skills training.	Identify common security roles with appropriate salary streams as guidance for agencies to ensure a uniform approach to security resourcing across the public sector and to assist with the attraction and retention of skilled staff within the state's Cyber Security workforce by 31 December 2018.		December 2019
3.2	Establish a leading Cyber Security Operations Centre.	Review the options available for a State Cyber Security Operations Centre and report to the ICT and Digital Governance Board. State Cyber Security Operations Centre established.	 	Completed August 2018 June 2021
3.3	Research and provide common services and tools for cyber security for use by government and non-government stakeholders.	Appropriate across government Cyber Security services and tools developed and endorsed by stakeholders.		December 2019
3.4	Facilitate growth and innovation in cyber security with other industries.	Areas (e.g. automation, artificial intelligence, cognitive computing, robotics) in which the state can facilitate growth and innovation identified during 2018 to 2021.		

 Delayed
 Strong Progress
 Ongoing
 Completed

#	Activity	Success Criteria	Progress	Due
3.5 ***NEW***	*Develop a cyber security pathway and promote cyber security as a career path.*	*Establish the new Certificate IV in Cyber Security Traineeship pathway for State Government.* *Support initiatives such as South Australian Cyber 'Schools Challenge' to increase student participation in Cyber Security.* *Work with SACE Board and Department of Education to develop Cyber Security as a core curriculum subject.*		December 2019
SR4 - Assess societal impacts				
4.1	Extend cyber security awareness to citizens via media and community engagement to create a valued cyber security conscious state.	Public media campaign established. Multi-year media and public relations campaign considered for launch in 2019.		June 2019
4.2	Support community programs to raise awareness about the impact of emerging risks, vulnerabilities and developing resilience.	Cyber security information regularly given to citizens via SA.GOV.AU. Regular drop in sessions for the public to ask cyber-related questions provided by 2019. The SA Government's community resilience strategy to include cyber threats, and the reliance on ICT.		
4.3	Include cyber security threats in the government's emergency management public awareness campaigns.	Inclusion of cyber security incidents on the 'emergencies and safety' section of SA.GOV.AU. Cyber security threats promoted at the State Emergency Management Committee via regular briefings and provision of security threat reports.		Completed January 2019

 Delayed
 Strong Progress
 Ongoing
 Completed

Contact

ICT and Digital Government, Office for Cyber Security
Department of the Premier and Cabinet
Government of South Australia
www.dpc.sa.gov.au

GPO Box 2343
Adelaide SA 5001

For further information relating to the South Australian Cyber Security Strategy 2018-2021 Annual Update 2019 please visit www.digital.sa.gov.au or email officeforcybersecurity@sa.gov.au

Government of South Australia

SOUTH AUSTRALIA