# South Australian Government

# CYBER SECURITY STRATEGIC PLAN 2018-2021

Government of South Australia

SOUTH AUSTRALIA

# CONTENTS

# STRATEGIC DIRECTION

Given the South Australian Government's critical role in service delivery, it is imperative that state infrastructure, digital assets and citizen information are adequately safeguarded against the ever-increasing incidence of cybercrime and espionage.

The Department of the Premier and Cabinet (DPC) is tasked with this responsibility, leading the delivery of this Cyber Security strategic Plan 2018-21 on behalf of the South Australian Government.

In consultation with other agencies and experts within the cyber security sector, DPC has developed this plan detailing the activities that will provide the South Australian Government with a stronger cyber security position. This will help deliver more responsible data sharing for social change, better protect the safety and prosperity of South Australians, and enhance the government's digital engagement with the business community.

A series of strategic objectives have been set to help achieve these desired outcomes:

- The government's infrastructure, services and systems are resilient to cyber threats.
- The government's digital and innovation agenda is empowered through a strong risk culture.
- Citizen's trust and confidence in the government's digital services is maintained through measured improvements in cyber security maturity.
- The cost and disruption to recover from cyber security incidents is minimised.
- Cyber security is managed in a way that meets industry and community expectations.
- Industry is motivated to invest, stimulating the state's economy and helping establish South Australia as a recognised cyber security leader in the Asia-Pacific region.

The plan's activities are structured within three strategic themes.

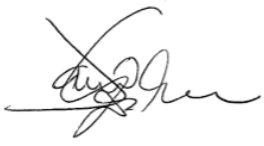
1. **Influence Leadership**
   Strengthen the role of government in providing sound governance and clear accountabilities for a whole of government approach to cyber security.
2. **Build Resilience**
   Strengthen the approach to the prevention of, detection of, response to and recovery from cyber security threats and incidents.
3. **Share Responsibility**
   Cultivate a collaborative approach that brings together all levels of government with academia and the private sector to cyber security.

In line with *SA Connected*, the South Australian Government's ICT strategy, our approach is to gain the benefits of innovation by embracing opportunities, informing our choices, and managing risks in an agile way.

Endorsed by

**Dr Don Russell**
Chair, Senior Management Council
Chief Executive, Department of the Premier and Cabinet
Government of South Australia

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



**Mr David Goodman**
Chief Information Security Officer
Government of South Australia

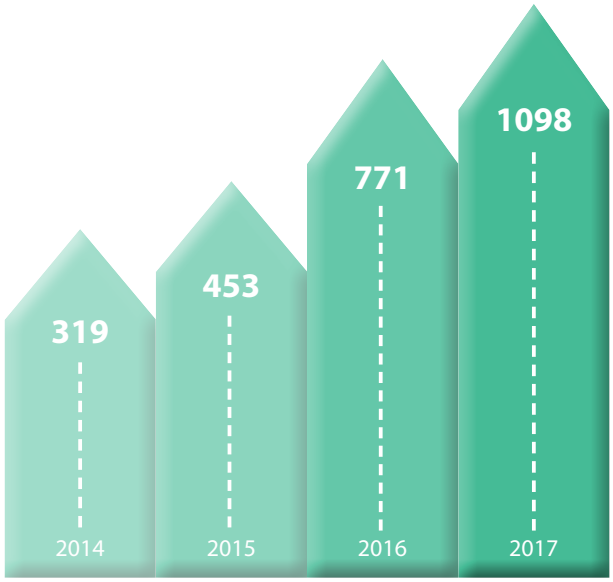
# SOUTH AUSTRALIAN CONTEXT

Driven by the Premier's Digital by Default Declaration that commits the government to a transformative agenda, the South Australian (SA) Government's approach to ICT ownership, management and delivery is undergoing significant change.

As more government services transition to digital platforms, the risk of cyber security incidents grows with the ability to impact service delivery, cause economic loss and harm the public's confidence in government services.

Data from SA's Cyber Security Incident Reporting Scheme supports this trend.

**Annual Cyber Security Reports in SA Government**




Total reports to Across Government Cyber Security Scheme

From a service delivery perspective, there has been an increased reliance on cloud services and managed service providers to deliver services to government agencies and the broader community.

With most agencies connected to a single network, an incident in one agency has the potential to rapidly affect all agencies, putting citizen services at risk. Fortifying internal policies and practices will help address this vulnerability.

Consistency across agencies is another challenge, evidenced by differing online environments, diverse risk profiles and varied information security expertise. Acknowledging that our capability and capacity need to increase, we need to continue to collaborate with the private sector and other stakeholders to stay abreast of security trends and further develop the skill sets of ICT professionals across government.

The SA Government supports the themes and ambitions within the Australian Government's Cyber Security Strategy launched in 2016. Collaboration at a national level and with industry partners is a key component of our approach to cultivate a collaborative approach to cyber security.

# ACTION PLAN

## 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.
- 1.2 Review the appropriateness and currency of existing cyber security policies for SA Government.
- 1.3 Implement a continuous improvement program and report regularly to the Senior Management Council on cyber security progress.

**IL2 - Lead people and change to improve the culture of cyber security**

- 2.1 Deliver employee training and build awareness about information security.
- 2.2 Integrate cyber risks within enterprise risk management processes.
- 2.3 Encourage trust and confidence in online and digital service delivery.
- 2.4 Support government agencies to ensure employees in positions of trust are appropriately trained and vetted.

**IL3 - Assign government responsibility**

- 3.1 Establish an across government Cyber Security Governance Committee.
- 3.2 Re-establish the across government IT Security Adviser Forum.
- 3.3 Develop a cyber security profession career path for SA Government.
- 3.4 Take an active role in leading and influencing national cyber security initiatives.

**IL4 - Measure cyber security performance**

- 4.1 Create a Balance Scorecard for security outcomes.
- 4.2 Support a risk-based prioritisation of government expenditure on cyber security.

## 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.
- 1.2 Deliver the ongoing SA Government Top Ten Cyber Resilience and Preparedness Objectives work program.
- 1.3 Develop a whole of government approach for the management of contractual cyber security risks.
- 1.4 Develop an external/internal vulnerability scanning and assessment capability.
- 1.5 Consciously consider emerging cyber threats in the development of intelligence products.
- 1.6 Improve security and policy control measures for areas of high risk, including critical infrastructure.
- 1.7 Develop a cyber security 'Marketplace' or 'Kiosk'.
- 1.8 Undertake regular cyber crisis planning, preparedness and response exercises with government and industry partners.

**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.
- 2.2 Review cyber insurance arrangements for government.
- 2.3 Create systems and processes for resource pooling for significant cyber security incident responses.

**BR3 - Grow**

- 3.1 Document and share lessons learned from significant cyber security incidents to promote cross-sector collaboration.
- 3.2 Establish uniformity of cyber security resourcing across the public sector to ensure adequate resourcing.

## 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.
- 1.2 Continue to develop the Watch Desk facility as a respected and leading incident detection, response and advisory group for across government.

**SR2 - Develop partnerships**

- 2.1 Support the establishment of the SA node of AustCyber.
- 2.2 Support the establishment of the Joint Cyber Security Centre in Adelaide.
- 2.3 Establish strong and improved engagement programs and partnerships with industry.
- 2.4 Establish partnerships with academia to ensure suitable education and training is available within SA for cyber security skills growth.

**SR3 - Build capability**

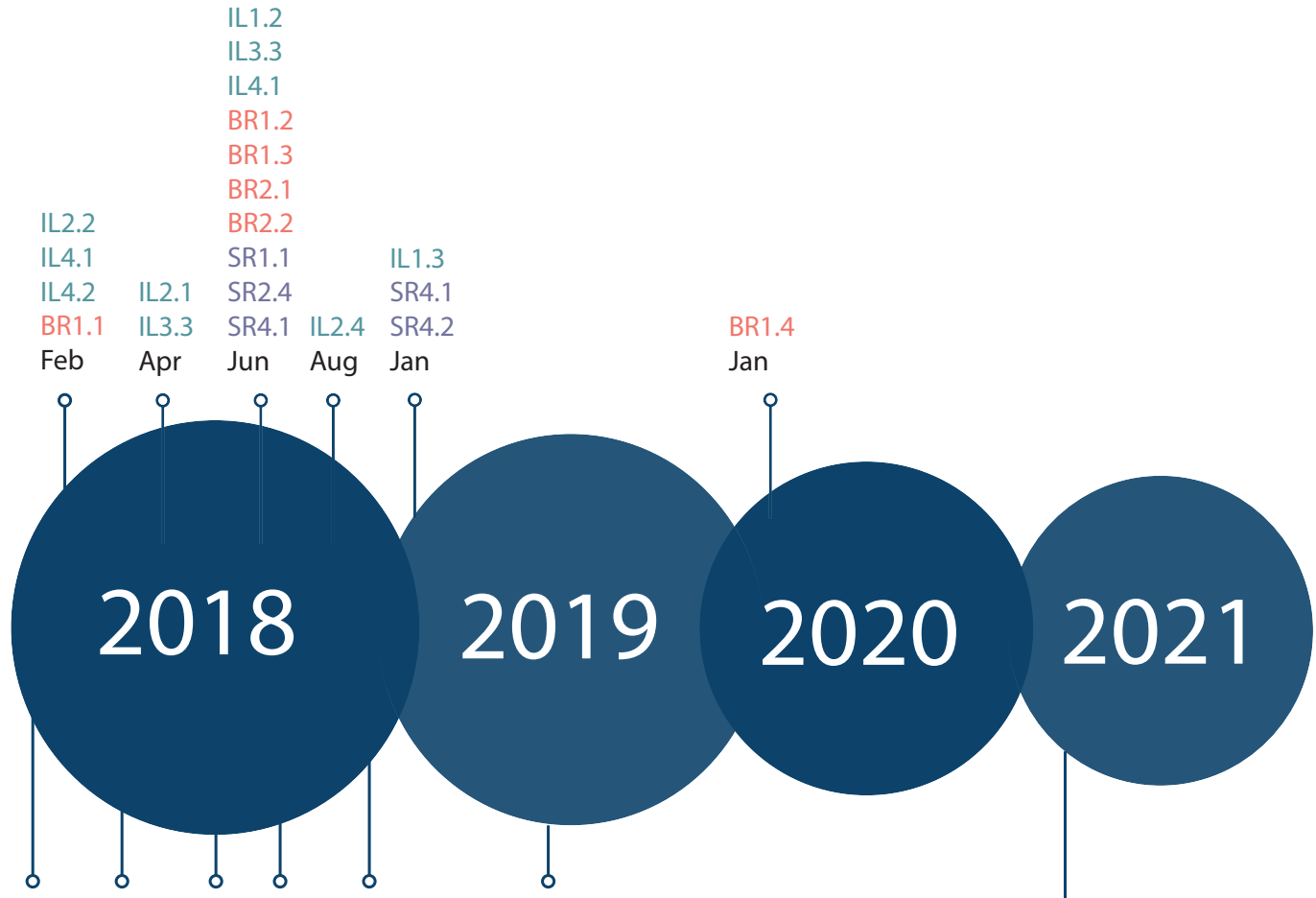
- 3.1 Ensure an agile future resource capability by providing appropriate skills training.
- 3.2 Establish a leading Cyber Security Operations Centre.
- 3.3 Research and provide common services and tools for cyber security for use by government and non-government stakeholders.
- 3.4 Facilitate growth and innovation in cyber security with other industries.

**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.
- 4.2 Support programs to raise awareness about the impact of emerging risks, vulnerabilities and developing resilience.
- 4.3 Include cyber security threats in the government's emergency management public awareness campaigns.

# TIMELINE

The first 12 to 18 months of the strategy will see a significant amount of work undertaken across three strategic themes. This initial period will form the foundation for the future deliverables and inform the first strategic plan review in early 2019.




Jan 2018 to Jan 2021 - IL2.3, IL3.4, BR1.5, SR2.3, SR3.3, SR3.4

**Strategic Themes**

**1: Influence Leadership**

**2: Build Resilience**

**3: Share Responsibility**

# STRATEGIC THEMES

## 1: Influence Leadership

Strengthen the role of the government in providing sound governance and clear accountabilities for a whole of government approach to cyber security.

| IL1 – Plan and develop policy frameworks | | |
|---|---|---|
| **Strategic Objective** | **Activity** | **Success Criteria** |
| *Align the South Australian Government Cyber Security Strategic Plan to Australia's Cyber Security Strategy.* | IL1.1 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. |
| | IL1.2 Review the appropriateness and currency of existing cyber security policies for the South Australian Government. | Information Security Management Framework (ISMF) 3.3 to be replaced by a simplified ISMF 4.0, and all associated standards and guidelines reviewed and updated by 30 June 2018.<br>Deliver Cloud Security standards and guidelines by 30 June 2018.<br>Deliver an updated PC030 – Protective Security Management Framework by June 2018.<br>Deliver an updated StateNet Conditions of Connection 4.0 by June 2018. |
| | IL1.3 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.<br>Strategic Plan reassessed and modified in January 2019. |

| IL2 – Lead people and change to improve the culture of cyber security | | |
|---|---|---|
| **Strategic Objective** | **Activity** | **Success Criteria** |
| *Provide strategic leadership to develop the capability to adapt in the face of new and emerging cyber security risks and threats.* | IL2.1 Deliver employee training and build awareness about information security. | An across government cyber and information security employee training and awareness package designed by April 2018.<br>A high proportion of employees complete the training.<br>An increased number of agencies adopt a mandatory induction and ongoing awareness program. |
| | IL2.2 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 by February 2018.<br>Advice is provided to agency audit and risk committees on cyber security risk strategies and frameworks. |
| | IL2.3 Encourage trust and confidence in online and digital service delivery. | A reporting template and guidance for security considerations delivered by June 2018.<br>A reduced number and impact of security incidents related to online and digital delivery of services by 2019.<br>Full mandatory integration of security considerations in design and implementation of online services by 2020. |
| | IL2.4 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.<br>Mandatory personal vetting and security screening implemented at a level appropriate to role prior to employment by August 2018.<br>Mandatory security training for staff employed in positions of trust by August 2018. |

| IL3 – Assign government responsibility | | |
|---|---|---|
| **Strategic Objective** | **Activity** | **Success Criteria** |
| *Provide oversight that clearly defines accountabilities and responsibilities for cyber security.* | IL3.1 Establish an across government Cyber Security Governance Committee. | An across government Cyber Security Advisory Sub Committee of the ICT and Digital Governance Board established.<br>Sub Committee established with industry representation by January 2018. |
| | IL3.2 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. |
| | IL3.3 Develop a cyber security profession career path for SA Government. | Defined role guidance for across government security personnel designed by March 2018.<br>An across government mentoring and secondment program established by June 2018.<br>Partnerships with industry and academia established to deliver relevant and suitable training for cyber and information security by April 2018. |
| | IL3.4 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.<br>Support the Joint Cyber Security Centre program and launch of the centre. |

| IL4 – Measure cyber security performance | | |
|---|---|---|
| **Strategic Objective** | **Activity** | **Success Criteria** |
| *Investment for Cyber Security is strategic and risk based whereby exposures are prioritised to ensure cyber security maturity is strengthened.* | IL4.1 Create a Balance Scorecard for security outcomes. | Independent across government cyber security assessment undertaken by February 2018.<br>Baselines for cyber security metrics set by February 2018.<br>Desired state for Cyber Security maturity defined for government agencies by June 2018. |
| | IL4.2 Support a risk-based prioritisation of government expenditure on cyber security. | Current levels and patterns of expenditure in cyber security across SA Government assessed by February 2018.<br>Use of economies of scale through across government procurement of cyber services increased by 2021. |

## 2: Build Resilience

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

| **BR1 – Prevent and prepare** | | |
|---|---|---|
| **Strategic Objective** | **Activity** | **Success Criteria** |
| *Increase preparedness for new and emerging cyber security threats to provide cyber resilience.* | BR1.1 Continue to develop the SA Government's cyber resilience position. | Independent Cyber Resilience Review undertaken by February 2018 (refer to IL4.1).<br>Participation in Australian Government Cyber Resilience activities to ensure alignment with state and national activities. |
| | BR1.2 Deliver the ongoing SA Government Top Ten Cyber Resilience and Preparedness Objectives work program. | Top 10 Cyber Resilience and Preparedness Objectives second report submitted to Cabinet by June 2018.<br>Continuous improvement cycle for monitoring and analysing data becomes common practice and is fed into policy and process decision making. |
| | BR1.3 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. |
| | BR1.4 Develop an external/ internal vulnerability scanning and assessment capability. | Full program implementation and business process established by January 2020. |
| | BR1.5 Consciously consider emerging cyber threats in the development of intelligence products. | Watch Desk continues to develop its holistic threat intelligence capability.<br>Watch Desk provides timely and accurate cyber threat and intelligence information with regular feedback sought from stakeholders.<br>Delivery of the threat intelligence sharing platforms (refer to SR1.1) |
| | BR1.6 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 by January 2018.<br>State Government Critical ICT Infrastructure program redeveloped by March 2018. |

| | | |
|---|---|---|
| | BR1.7 Develop a cyber security 'Marketplace' or 'Kiosk'. | Economies of scale achieved through across government procurement of essential cyber security tools/services by July 2018. |
| | BR1.8 Undertake regular cyber crisis planning, preparedness and response exercises with government and industry partners. | An annual training program delivered each year.<br>Cyber Terrorism exercise (funded by Australia-New Zealand Counter Terrorism Committee) undertaken by March 2018. |

| **BR2 – Respond and recover** | | |
|---|---|---|
| **Strategic Objective** | **Activity** | **Success Criteria** |
| *Proactively ensure the state's cyber security arrangements deliver better outcomes for the state.* | BR2.1 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.<br>SA Government response arrangements aligned with the Australian Government cyber crisis management arrangements by June 2018. |
| | BR2.2 Review cyber insurance arrangements for government. | Cyber Insurance arrangements reviewed by June 2018. |
| | BR2.3 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).<br>SA Communications Sector Forum's capability and capacity developed through awareness raising exercises. |

| BR3 – Grow | | |
|---|---|---|
| **Strategic Objective** | **Activity** | **Success Criteria** |
| *Undertake continuous improvement to further understand the impact of cyber security incidents and provide uniformity of cyber security resourcing across agencies.* | BR3.1 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.<br>Lessons learnt are shared as required and on a quarterly basis thereafter – with a process in place by January 2018. |
| | BR3.2 Establish uniformity of cyber security resourcing across the public sector to ensure adequate resourcing. | Cyber Security Workforce Framework developed by December 2018. |

## 3: Share Responsibility

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 | | |
|---|---|---|
| **Strategic Objective** | **Activity** | **Success Criteria** |
| *Establish trusted partnerships for threat intelligence and knowledge sharing across the cyber security community.* | SR1.1 Deploy a Threat Intelligence Platform for use by all government agencies. | Cyber Threat Intelligence Sharing Toolkit deployed for agency use by January 2018.<br>Toolkit deployed for private sector partners by June 2018. |
| | SR1.2 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 January 2018. |

| SR2 – Develop partnerships | | |
|---|---|---|
| **Strategic Objective** | **Activity** | **Success Criteria** |
| *Strengthen and enhance cyber security resilience and build the capacity of SA Government through improved engagement programs, collaboration of resources, intelligence and partnerships.* | SR2.1 Support the establishment of the SA Node of AustCyber. | SA Node established by January 2018. |
| | SR2.2 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. |
| | SR2.3 Establish strong and improved engagement programs and partnerships with industry. | Partnerships and engagement programs established and continuously improved to achieve optimal outcomes for stakeholders.<br>Ongoing support for the work of the Australian Government Critical Infrastructure Centre.<br>Ongoing support for the Trusted Information Sharing Network model, including participation in appropriate governance groups and involvement in exercises and training. |
| | SR2.4 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.<br>Examine support for the Cyber Security Cooperative Research Centre, with potential opportunities identified by June 2018. |

| SR3 – Build capability | | |
|---|---|---|
| **Strategic Objective** | **Activity** | **Success Criteria** |
| *Develop the capability to adapt and be responsive in the face of new and emerging cyber security threats.* | SR3.1 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. |

| | | |
|---|---|---|
| | SR3.2 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 by March 2018.<br>State Cyber Security Operations Centre established by June 2019 (linked to SR1.3). |
| | SR3.3 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. |
| | SR3.4 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. |

| **SR4 – Assess societal impacts** | | |
|---|---|---|
| **Strategic Objective** | **Activity** | **Success Criteria** |
| *Educate South Australians about the impact of new and emerging cyber security threats, risks and how to develop resilience.* | SR4.1 Extend cyber security awareness to citizens via media and community engagement to create a valued cyber security conscious state. | Public media campaign established by June 2018.<br>Multi-year media and public relations campaign considered for launch in 2019. |
| | SR4.2 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.<br>The SA Government's community resilience strategy to include cyber threats, and the reliance on ICT. |
| | SR4.3 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 by March 2018.<br>Cyber security threats promoted at the State Emergency Management Committee via regular briefings and provision of security threat reports. |

# RELATED DOCUMENTS

The South Australian Government Cyber Security Strategic Plan 2018-21 builds upon the following documents.

Australia's Cyber Security Strategy
SA Connected – SA Government's ICT strategy
Digital by Default Declaration
State Emergency Management Committee Strategic Framework 2017-2022
South Australia's Seven Strategic Priorities
South Australia's Economic Priorities

## Contact

Office for Cyber Security
Department of the Premier and Cabinet
Government of South Australia

www.digital.sa.gov.au
www.dpc.sa.gov.au

GPO Box 2343
Adelaide SA 5001

For further inquiries please contact:
ciso@sa.gov.au

Government of South Australia

SOUTH AUSTRALIA