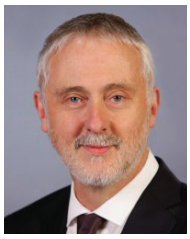
CYBER SECURITY STRATEGY

VICTORIA

Contents

MESSAGE FROM THE SPECIAL MINISTER OF STATE



Victorians expect government services to be reliable and their information kept secure.

Our economy relies on fast and secure telecommunications, secure and trustworthy data, secure infrastructure, and core services that are always available. At the same time, the Government and its partner service providers use technology and information to support operations, make decisions, and deliver services to Victorians.

Our systems, infrastructure and approach to security need to be resilient in the face of increasing cyber security threats. The government intends to deliver its existing and new digital services securely.

Traditional cyber security approaches have focussed on prevention controls and compliance standards. These have an important place, but it is evident that an expanded focus is needed on cyber security incident monitoring, detection, response, and recovery capabilities. This expanded concept of *cyber resilience* is the ability to prepare for, respond to and recover from cyber incidents and disruption.

Further, we recognise that our people need to be skilled and held accountable for making cyber security part of the fabric of government data and information management. And this uplift in thinking and capability needs focus and leadership.

This 23-point strategy outlines the steps we are taking to improve cyber resilience, governance and approach both within government and with Victoria's major infrastructure and service providers. It relies on collaboration across governments, across service providers, with the university sector and with Victoria's vibrant technology sector.

Establishing and maintaining Victoria's cyber resilience will be a long-term challenge requiring an ongoing commitment. The Government is prepared to meet that challenge.

Gavin Jennings
Special Minister of State

VISION

SECURE AND RESILIENT GOVERNMENT INFORMATION, SERVICES, AND INFRASTRUCTURE

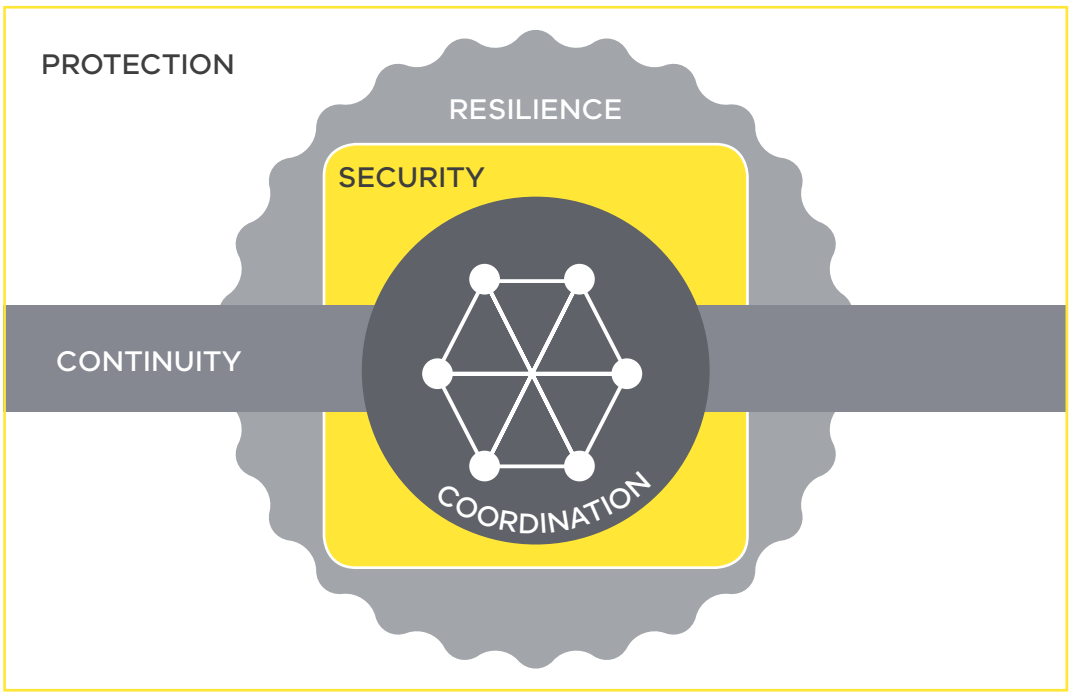
DEFINITION

Cyber security refers to measures relating to the confidentiality, availability and integrity of information and data that is processed, stored and communicated by electronic or similar means, protecting it and associated systems from external or internal threat.

PURPOSE

To develop and implement cyber security capabilities to preserve and improve the:

- protection of sensitive citizen and other data against loss, malicious alteration, and unauthorised use
- resilience of government services, systems and infrastructure to cyber threats
- continuity of government during and following serious cyber incidents
- protection and security of new digital services for citizens
- coordination of our response to threats against infrastructure
- security and viability of Victorian Government core infrastructure.



PRINCIPLES

Collaborative

The Victorian Government, the Australian Government, and the private sector will share security information to improve outcomes and save effort and resources

Enabling

Stronger cyber security will support safe and secure use of current, new and innovative technologies, allowing government to conduct business confidently in a contemporary world

Proven

Cyber security capabilities will be developed or acquired based on sound evidence and tested for their effectiveness and applicability

Scalable

Cyber security services and capabilities will be deployed widely and offered to the Victorian public service

Proportional

Cyber security resources will be focused on increasing the resilience of high value assets and systems: Resources will be focused on increasing the resilience of high value assets and systems, proportional and based on sound risk assessment.

Sustainable

Cyber security is an escalating long-term challenge that requires a continuous improvement program supported with appropriate resourcing, education and training

CONTEXT

The *Victorian Government Information Technology Strategy* released in May 2016 called for the development of a cyber security strategy. The *IT Strategy* highlighted that the security of information and infrastructure is essential to the functioning of government.

Secure and resilient information and services safeguard the State's economic growth, productivity, and competitiveness.

Threat environment

Government networks in Australia are regularly targeted by the full breadth of cyber adversaries. Yet, relatively few organisations have sufficiently planned or prepared for a significant cyber security incident.

In recent decades there has been a shift from relatively unsophisticated lone actor cyber-attackers towards organised crime, funded political 'hacktivists' and even foreign governments using cyberspace as a means to infiltrate government, business, and private networks. The motivations range from political influence, vandalism, theft, extortion and the subverting of government processes and data for personal or broader reasons.

The methods used are evolving and increasing in sophistication, employing both technical and social engineering attack vectors to attempt to steal data, alter systems, extort money, disrupt government programs, undermine businesses, and cause distress to citizens.

The scale of incidents and disruption is unprecedented. Government is continually working to keep up – and new tools are improving our understanding of the magnitude of incidents we experience daily.

The threat environment we face is increasing at all levels of government and against every system we operate. While our approach to date has worked to some extent, Victorian Auditor-General reports and departmental in-house testing regularly uncover vulnerabilities that must be addressed. The time for an agency-by-agency (only) approach has passed. We need to address these risks strategically, and where it makes sense, holistically.

Government

Cyber resilience is essential to maintain and enable government service delivery, digital engagement, and public sector reform.

Victorian Government services are delivered by discrete departments and agencies that are accountable for their respective operational environments. These agencies make cyber security investments that reflect their specific risks and needs. The opportunity for the Government as a whole is to build and sustain strong cyber security capabilities across all agencies.

Cyber security capability across the public sector needs to be improved. It should be consistent, less fragmented, based on industry practice, and appropriate to the risk profile of each organisation. The importance of improving cyber security maturity across the public sector has been highlighted by successive information security-related reports from the Victorian Auditor-General.

Skills

The Government must compete with the public and private sectors for increasingly in-demand and expensive cyber workforce skills. Mature cyber security services require significant scale, automation, specialist skills, ready access to a broad range of cyber resources and ongoing investment.

Cyber resilience

Improved cyber security requires a spectrum of defences that build on the traditional approach of prevention controls and compliance with standards. Organisations at the forefront of cyber security recognise that there also needs to be a focus on detection, mitigation of vulnerabilities, and swift recovery. Together, these approaches are described as *cyber resilience*.

Cyber resilience means having appropriate internal cyber capability, strong governance and policy, strategic partnering, cyber situational awareness, ongoing cyber risk assessments (including understanding the risks and flow-on impact of a cyber breach), clear communication mechanisms, and a rapid cyber breach response capability. For example, cyber resilience means moving beyond the reading of log files after the fact and towards understanding network traffic in real time, and actively and consciously analysing user behaviours and data flows. Cyber resilience needs to be seen as a component of planning and preparedness.

APPROACH AND PARTNERS

We will appoint a Chief Information Security Officer for the Government within the Department of Premier and Cabinet (DPC). DPC will continue to source internal expertise via the whole-of-government *Information Security Advisory Group*, a subcommittee of the *Chief Information Officers Leadership Group*.

Government agencies and partners

The Privacy and Data Protection Deputy Commissioner (PDPDC) regulates three areas of activity:

- information privacy
- protective data security

The key functions with regard to protective data security and law enforcement data security are:

- to develop the Victorian Protective Data Security Framework (VPDSF)
- to issue protective data security standards and law enforcement data security standards
- to conduct monitoring and assurance activities to assess compliance with those standards
- to undertake research, issue reports, guidelines and other materials with regard to protective data security.

The VPDSF is the overall scheme for managing protective data security risks in Victoria's public sector. Cyber security strategy initiatives and deliverables will support the VPDSF principles and approach.

Emergency Management Victoria (EMV)

EMV is the overarching body for emergency management in Victoria. It has the lead role in maintaining and coordinating whole-of-government strategy and policy for critical infrastructure resilience to ensure a consistent approach across our state.

The Victorian Government released the *Critical Infrastructure Resilience Strategy* in July 2015.

The Strategy stated that the health, safety, and prosperity of Victorians are reliant on certain infrastructure. The complex, interconnected, and often interdependent nature of this critical infrastructure increases the risk of a disaster-causing systemic failure.

The strategy highlighted the growing cyber threat and the pervasive reliance on secure internet-connected control technologies. The potential economic, social, environmental, political, and national security costs of a cyber breach are significant. Cyber threats should be one of the emergency risks for which Victorian critical infrastructure owners and operators prepare.

Victorian Managed Insurance Authority (VMIA)

VMIA provides insurance against damage to state assets or liabilities to third parties arising from cyber incidents. The VMIA has an established capability to provide risk advice and insurance services for the Victorian Government.

Increased government agency participation in the cyber security planning cycle will be risk-based and developed and implemented in partnership with the VMIA.

To build Victorian Government risk management capability, the VMIA conducts training programs, seminars and educational events on current and emerging topics in insurance and risk management. DPC will partner with VMIA to expand the content of this training to include cyber security awareness.

CenITex

CenITex is the Victorian Government's shared services provider for information technology. It provides services to a range of departments, now including agencies that were not part of its initial remit.

A relevant example of the services CenITex provides are the recently-established security operations centre services. This strategy contains actions that will seek to leverage these services where it makes sense, and broaden them into a stronger more widely available service.

Australian Government

Victoria works actively with the Australian Government for advice and services. It receives cyber security intelligence from the Australian Cyber Security Centre (including the Australian Signals Directorate), and liaises with other Australian Government cyber security agencies.

Officers from the Australian Government were on the Strategy Group that assisted with the development of this Strategy.

CERT

CERT Australia is the national computer emergency response team. As part of Australia's Cyber Security Strategy, CERT is responsible for the National Cyber Security Exercise Program, and will manage the Government's participation in regular multi-agency cyber security exercising to build resilience, readiness, and capability.

The overarching objective of the program is to support continuous improvement through the maintenance, development, interoperability, and evaluation of Australia's nation-wide cyber security arrangements. The program will exercise at all levels to ensure both government and private entities have an improved understanding of how to engage across different levels of government, business, and industry to minimise the impact of cyber security incidents and disruptions.

In the development of the program, CERT Australia will be consulting with state and federal agencies, including Victoria, to ensure all cyber security exercising needs are addressed during the delivery of the program.

The Victorian Government will work with CERT Australia to ensure its participation as part of this Strategy.

Industry and academic partners

Victoria's economy is becoming more globally connected and our future growth is increasingly dependent on accessing international markets and attracting investment. The Government has an economic imperative to build cyber security capacity and to facilitate private sector involvement in this critical industry.

The Government is seeking to address some of these challenges and is targeting support for priority industry sectors through initiatives that seek to drive Victoria's economic growth and new job creation.

In the context of cyber security, the digital technology sector and innovation is a significant driving force for economic growth, productivity, and competitiveness. Digital technology will drive innovation and increase the competitiveness of the State's industries, developing advanced capabilities that will grow the economy.

Victoria must continue to adapt and innovate in an increasingly digitised society where science, technology, engineering, and maths (STEM) skills, digital literacy and numeracy are increasingly important.

The Victorian Government is committed to making Victoria the number one destination for digital technology companies and start-ups in the Asia-Pacific region. Victoria is leading the nation on cyber security, with the recent announcements of the establishment of CSIRO's Data61 Cybersecurity Innovation Hub, the Oceania Cyber Security Centre, the collaboration with Oxford University's Global Cyber Security Capability Centre, and a Melbourne-based node of the Commonwealth Government's Cyber Growth Centre. This hub of cyber security infrastructure will develop cyber skills, commercialise technology research and development, and drive private sector investment into the State's cyber security industry.

Oceania Cyber Security Centre

The Government has supported the establishment of the new Oceania Cyber Security Centre (OCSC) in Melbourne. The OCSC brings together eight Victorian universities and major private sector partners, to position Melbourne as a regional leader in cyber security education, research, policy, and entrepreneurship.

The OCSC aims to partner with industry to develop research and training opportunities for dealing with cyber security. Based at the Docklands Goods Shed precinct, the OCSC will work closely with other research collaborators and industries. Research specialists will be close to new ideas, new products new concepts; and as specialists in cyber security, they are better placed to anticipate the future of technology and the associated risks and rewards.

The OCSC will work with industry and government partners to provide advice on current and future security threats, to develop new technology and create commercialisation opportunities, to train staff and students on the latest techniques for protecting security. Areas of expertise include: Critical Infrastructure, the Internet of Things; Verification Security; Network Security; Advanced Cryptography; Big Data; and Automation and Industrial Control Systems.

OCSC is working with Israel's Tel Aviv University (TAU) to share resources to help companies better protect their data and privacy, and allow Victorian researchers to visit Israel and learn from some of the world's most experienced cybersecurity experts. They will work with TAU's Blavatnik Interdisciplinary Cyber Research Centre.

Oxford University

The Government has created a landmark agreement with Oxford University's world leading Global Cyber Security Capacity Centre (GCSCC) to establish a collaboration with OCSC to implement GCSCC's capability model to the Asia Pacific region.

Data61

With the support of the Government, Data61, the national digital research arm of CSIRO, located their lead national cyber security capability to Melbourne at the Data61 Cyber Security Innovation Hub, based at the Goods Shed, Docklands.

Cyber Security Growth Centre

As a result of the significant cyber security cluster developing in Victoria, the Commonwealth Government announced that the national Cyber Security Growth Centre will have two nodes, one of which will be Victoria housing at the Goods Shed together with OCSC and Data61.

AGENCIES, INDUSTRY AND ACADEMIC PARTNERS INCLUDE:

EMV EMERGENCY MANAGEMENT VICTORIA

vmia Risk Management and Insurance

CenITex

Australian Government

ACSC AUSTRALIAN CYBER SECURITY CENTRE

OCSC Oceania Cyber Security Centre

Global Cyber Security Capacity Centre

DATA 61

CSIRO

Approach

This 23-point strategy is organised under five priorities designed to uplift the cyber security capacity of the Government. These priorities are in response to the principles set out earlier (page 5).

ENGAGEMENT

Formal executive support and leadership is critical to achieving the required outcomes.

The state's cyber security challenges require a sustained focus and whole-of-Victorian-Government collaboration. Establishing and maintaining appropriate levels of cyber resilience is an ongoing and long-term challenge.

PLANNING

For most government entities, achieving and sustaining an appropriate level of cyber resilience is too complex a challenge to achieve on its own.

The co-operative three year planning cycle will provide the opportunity to identify use of shared and common services and build capability based on effective cyber expenditure, supporting sustainable outcomes.

PARTNERING

Government will leverage its relationships, its internal capability and industry expertise.

SERVICE MATURITY

Buying intelligently and mitigating identified capability gaps will lead to greater efficiency and stronger cyber resilience than the current piecemeal approach.

CAPABILITY

Cyber expertise and awareness are critical to preventing and reducing costly and disruptive cyber incidents.

Developing and maintaining the right balance between in-house cyber security skills and appropriate use of managed security services is required.

SECURE AND RESILIENT GOVERNMENT INFORMATION, SERVICES AND INFRASTRUCTURE

PRIORITY A – ENGAGEMENT

A clear understanding of the state's cyber security posture, risk profile and threat landscape allows decision-makers to make appropriate investment decisions. This understanding comes from clear accountabilities, regular high-quality reporting, and the establishment of a focal point for leadership within government.

Chief Information Security Officer

A Chief Information Security Officer (CISO) for Victoria will be appointed. This executive role will oversee government's response to the cyber threat, develop best practice, provide assurance, report internally on our cyber security status, and coordinate cross-government action. The CISO will be created within DPC, and will have a supporting staffed unit.

The CISO will not replace the individual responses and accountability within each government agency to address risks in the cyber landscape, nor will it assume responsibility within these agencies to address the standards issued by the Office of the Victorian Information Commissioner. Rather, the CISO will coordinate cross-government responses in those areas where a whole-of-government approach is preferable, more efficient and will provide better security outcomes than individual approaches – for example, the creation of whole-of-government cyber services, capabilities, reporting, executive engagement, and information dissemination.

The CISO will be the government executive responsible for delivering this Strategy.

Reporting and communication

The Government recognises that it requires frequent, high quality, and standardised reporting for senior executives. Government needs to be kept abreast of Victoria's risk profile and be given information that allows it to assess the adequacy of its cyber resilience, and for individual departments and agencies to do the same. Cyber security investment decisions need to be based on current credible evidence. This evidence and analysis will also support existing risk and attestation responsibilities for agency heads, and support cyber security risk being tracked within each agency.

This standardised reporting will include:

- cyber security threat assessment and current security posture
- cyber resilience maturity and gap analysis of departments and agencies
- opportunities for collaboration and shared cyber security services
- cyber security investment status
- cyber incident and breach summary.

Engagement outcomes

- Whole-of-government oversight and focus on cyber security resilience.
- Better and informed investment decisions at both a whole-of-government and agency level through a clear understanding of the Government's cyber security positioning.
- Cyber security becoming embedded into the normal operations of government through regular actionable communication and awareness programs.
- Clearer accountability and focus for agency heads in managing cyber security risk within their agencies.

ENGAGEMENT ACTIONS

	ACTION	DUE
1	Appoint a *Victorian Government Chief Information Security Officer* and establish a cyber security office	**September 2017**
2	Develop and present a quarterly cyber security briefing and status report to the Victorian Secretaries Board and the State Crisis and Resilience Committee	Every 3 months, from **September 2017**
3	Develop and operate a communication and engagement program for cyber security awareness within government	From **December 2017**

PRIORITY B – PLANNING

A planning cycle creates a rhythm for strategic action – away from the tactical responses needed for day-to-day incident and threat management. It helps identify the appropriate use of shared and common services, and builds capability to support sound investment and sustainable response mechanisms.

This planning approach will build on existing governance structures, compliance requirements, operational responsibilities, and risk management accountabilities. This ensures the approach is cost-effective, sustainable, and will achieve an appropriate level of cyber resilience.

A key component of the planning cycle will be to enable stakeholders to identify and agree on capability gaps that are most effectively addressed by either a shared or common service; or sourced from within government, the commercial market, or via a hybrid model.

The three-year planning cycle will be based on a commonly recognised cyber security capability maturity model. It will identify where to invest and act to improve cyber security resilience based upon informed, risk-based analysis aimed at the protection of priority services, assets and systems.

Planning will identify priority information and infrastructure assets, and determine the case for monitoring, detection, response, and recovery capabilities.

The planning methodology will reference the US-based National Institute for Science and Technology's Cyber Security Framework (CSF) taxonomy. The framework core consists of five concurrent and continuous functions – identify, protect, detect, respond, and recover.

The three-year planning cycle will comprise a baseline planning exercise, an eighteen-month cyber security operational health check and a series of annual plans. In addition to whole-of-government capability, the assessment process will enable each department and agency to define its own three-year cyber security target state, prioritise cyber security activities and make informed decisions about cyber security investment at the agency level.

Clearer cyber emergency governance arrangements are being developed in consultation with EMV. These will be implemented as a priority. This work will be undertaken with EMV and departments via established governance arrangements to ensure that cyber threats are one of the emergency risks considered by Victorian critical infrastructure owners and operators. Victoria's *Critical Infrastructure Resilience Strategy* acknowledges that compromise of industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, can result in a major disruption to community services.

Planning outcomes

- Disciplined approach to understanding and responding to the cyber security threat.
- Better informed investment decisions at a whole-of-government and agency level through a considered understanding of threats, priorities and response mechanisms.
- Improved information sharing and leveraging of internal capability through stronger engagement within the Government's cyber security community.
- Improved focus on planning and readiness for cyber attacks on ICS/SCADA systems.

Planning actions

	ACTION	DUE
4	Finalise implementation of cyber emergency governance arrangements, including the creation of a cyber security group reporting ultimately to the State Crisis and Resilience Committee	**October 2017**
5	Establish an initial baseline of cyber security status, including identifying high value information assets and infrastructure, followed by an annual cyber resilience benchmark report and status of progress against strategy delivery	Every 12 months from **November 2017**
6	Identify and promote common cyber security services that can be accessed and shared	Every 12 months from **March 2018**
7	Establish an ICS/SCADA cyber security working group reporting ultimately to the State Crisis and Resilience Council that will develop and implement a three year multi-agency cyber security exercising program to build resilience, readiness, and capability	**September 2017**
8	Describe cyber security desired target state	Every 3 years from **September 2017**
9	Undertake cyber security operational health check	Every 12 months from **June 2018**
10	Undertake desktop target state review (timing meshes with Action 8)	Every 18 months from **March 2019**

PRIORITY C – PARTNERING

No single agency can address the threat to cyber security on its own. Partnering across departments leverages government's combined capability, but even this is not enough.

The Government recognises that it needs to combine forces both within government and with the private sector. We know that strong partnerships benefit all participants. A combined strategic approach, intelligence sharing, capability sharing, and the capacity to test proposed approaches with leading cyber industry practitioners, all add value.

We know that there are services and expertise that we need to procure at points in time and for ongoing services.

There are specialist agencies and services within government that can assist agencies and the Government as a whole. The Australian Government is also working to increase its own capability and capacity to assist other governments across our nation.

We have already established a Cyber Security Strategy Group to assist in the development of this strategy. This group will continue, with consideration being given to broaden its membership (see "Cyber Security Strategy Group" at the end of this document). We will build on this to establish intelligence-sharing and better practice mechanisms.

We will continue to partner with the Australian Government both for services and strategic planning. Victorian Government agencies such as PDPDC, VMIA, EMV and CenITex form part of the spectrum of related functions that help government address cyber threats.

We will boost our own cyber security capabilities with established private sector cyber security services, partnering with academia, and through other intelligence-sharing bodies, for example the newly established Oceania Cyber Security Centre.

Partnering outcomes

- Greater insight and increased timeliness through shared intelligence.
- Better practice through engagement with cyber security experts within the Victorian Government, specialist Victorian Government agencies, the Australian Government, industry, and academia.
- A holistic approach and broader capability arising from targeted and strategic vendor relationships.

Partnering actions

ACTION		DUE
11	Establish Cyber Security Strategy Group to facilitate a cross-industry strategic approach and an intelligence sharing mechanism	Strategy group commenced: **August 2016** Intelligence sharing mechanism: **October 2017**
12	Establish formal channels and mechanisms to engage with Australian Government cyber security services and strategic planning	Commenced: **August 2016**
13	Establish a procurement panel to access private sector cyber services	**June 2018**
14	Identify high inherent risk in small and medium sized entities (in conjunction with VMIA) so that services can be targeted	**December 2017**
15	Establish (with VMIA) a cyber capability uplift program including cyber security training, educational events, programs, and seminars	**March 2018**
16	Work with CERT to align with the National Cyber Security Exercise Program initiative stemming from Australia's Cyber Security Strategy	**October 2017**

PRIORITY D – SERVICE MATURITY

The Victorian Government uses services provided by the cyber security industry to enhance and supplement our in-house capability.

The procurement of some services has typically been undertaken at the department and agency level. This will continue.

However, there are a number of services that make sense for the Government to procure on a whole-of-government basis. Through the development of this strategy, and based on already-recognised opportunities, a number of services have already been put into place; and others have been identified.

An example of an existing service is the Victorian Government information sharing and incident response service.

The next step is for government to address its purchased and in-house cyber security maturity. Including:

- rationalising and co-ordinating the procurement of cyber security services
- developing a federated Victorian Government Security Operations Centre service model plan (which takes into account in-house capability, including that being developed at CenITex)
- developing a small and medium size agency cyber security operational model.

Careful consideration needs to be given to developing and maintaining the right balance between in-house cyber security skills and appropriate use of managed security services. The Government needs to be a smart buyer and consumer of cyber security services and maximise the opportunity to develop and retain its own cyber security skilled workforce.

Government needs to address the cyber resilience challenge strategically and collaboratively. This allows us to maximise our investment and allows agencies access to functional capabilities that will allow them to meet a challenge that is too complex for any one agency to deal with on its own.

Further, incidents can be multi-agency in scope. The effective management of a multi-agency incident through a supplier that operates across the government as a whole can greatly decrease the severity, scope, damage and cost of a cyber security incident.

Service maturity outcomes

- Incident response and recovery are enhanced, and multi-agency threats are recognised earlier, when an integrated federated Security Operations Centre capability is deployed.
- Long term service maturity is established through increased in-house capability.
- Better information technology and business systems investment decisions are made when guidance and initial assessments for consuming cloud services are available.
- Improved understanding and quantification of the potential impact of a cyber breach.
- Costs efficiency through a shared approach to establishing and developing cyber capabilities.

SERVICE MATURITY ACTIONS

ACTION		DUE
17	Establish and maintain a Victorian Government information sharing and incident response service comprising of contract arrangements and appropriate onsite service providers	Underway, from **September 2016**
18	Determine and establish whole-of-government subscriptions for internet security and information security services	**September 2017**
19	Develop an integrated and federated Security Operations Centre model and implementation plan	**February 2018**
20	Undertake an assessment and issue guidance in relation to the Government's obligations as a customer when consuming cloud services in a shared security model	**November 2017**
21	Develop and pilot a small and medium organisation cyber security operational model	**April 2018**

PRIORITY E – CAPABILITY

Government recognises that a multi-level approach to skills development, skills attraction, and general cyber security awareness is needed. Not only are specialist skills required, but there is a need to uplift cyber security awareness and training for all government employees.

Specialist cyber security skills are in high demand. Agencies have limited in-house cyber security skills and face difficulties in retaining expertise. Improving internal specialist cyber security capabilities will be based on a mix of in-house development and service augmentation from the market. In some cases, certain cyber security services will be most efficiently provided by a single source, allowing for specialisation and better concentration and coordination of scarce resources.

The Government requires a cyber security specialist workforce plan. It is expected that this will need to be developed with the education sector; partnering with universities and specialist educators like the Oceania Cyber Security Centre.

Capability outcomes

- Productivity improvement due to a reduction in outages and loss of data, which will come from an increase in the general capability of all public service employees around cyber security
- Increased resilience in cyber security arising from an end-to-end focus on developing in-house specialist cyber security capability

CAPABILITY ACTIONS

	ACTION	DUE
22	Commence implementation of the cyber security capability recommendations released as part of the IT Capability Uplift Plan and developed under the *Victorian Government IT Strategy*	**March 2018**
23	Develop a workforce plan to attract, develop and retain specialist cyber security skills	**March 2018**

COMPLETE SET OF ACTIONS

ENGAGEMENT

	ACTION	DUE
1	Appoint a *Victorian Government Chief Information Security Officer* and establish a cyber security office	**September 2017**
2	Develop and present a quarterly cyber security briefing and status report to the Victorian Secretaries Board and the State Crisis and Resilience Committee	Every 3 months, from **September 2017**
3	Develop and operate a communication and engagement program for cyber security awareness within government	From **December 2017**

PLANNING

	ACTION	DUE
4	Finalise implementation of cyber emergency governance arrangements, including the creation of a cyber security group reporting ultimately to the State Crisis and Resilience Committee	**October 2017**
5	Establish an initial baseline of cyber security status, including identifying high value information assets and infrastructure, followed by an annual cyber resilience benchmark report and status of progress against strategy delivery	Every 12 months from **November 2017**
6	Identify and promote common cyber security services that can be accessed and shared	Every 12 months from **March 2018**
7	Establish an ICS/SCADA cyber security working group reporting ultimately to the State Crisis and Resilience Council that will develop and implement a three year multi-agency cyber security exercising program to build resilience, readiness, and capability	**September 2017**
8	Describe cyber security target state	Every 3 years from **September 2017**
9	Undertake cyber security operational health check	Every 12 months from **June 2018**
10	Undertake desktop target state review (timing meshes with Action 8)	Every 18 months from **March 2019**

PARTNERING

	ACTION	DUE
11	Establish Cyber Security Strategy Group to facilitate a cross-industry strategic approach and an intelligence sharing mechanism	Strategy group commenced: **August 2016** Intelligence sharing mechanism: **October 2017**
12	Establish formal channels and mechanisms to engage with Australian Government cyber security services and strategic planning	Commenced: **August 2016**
13	Establish a procurement panel to access private sector cyber services	**June 2018**
14	Identify high inherent risk of small and medium sized entities (in conjunction with VMIA) so that services can be targeted	**December 2017**
15	Establish (with VMIA) a cyber capability uplift program including cyber security training, education events, programs, and seminars	**March 2018**
16	Work with CERT to align with the National Cyber Security Exercise Program initiative stemming from Australia's Cyber Security Strategy	**October 2017**

SERVICE MATURITY

	ACTION	DUE
17	Establish and maintain a Victorian Government information sharing and incident response service comprising of contract arrangements and appropriate onsite service providers	Underway, from **September 2016**
18	Determine and establish whole-of-government subscriptions for internet security and information security services	**September 2017**
19	Develop an integrated and federated Security Operations Centre model and implementation plan	**February 2018**

20	Undertake an assessment and issue guidance in relation to the government's obligations as a customer when consuming cloud services in a shared security model	**November 2017**
21	Develop and pilot a small and medium organisation cyber security operational model	**April 2018**

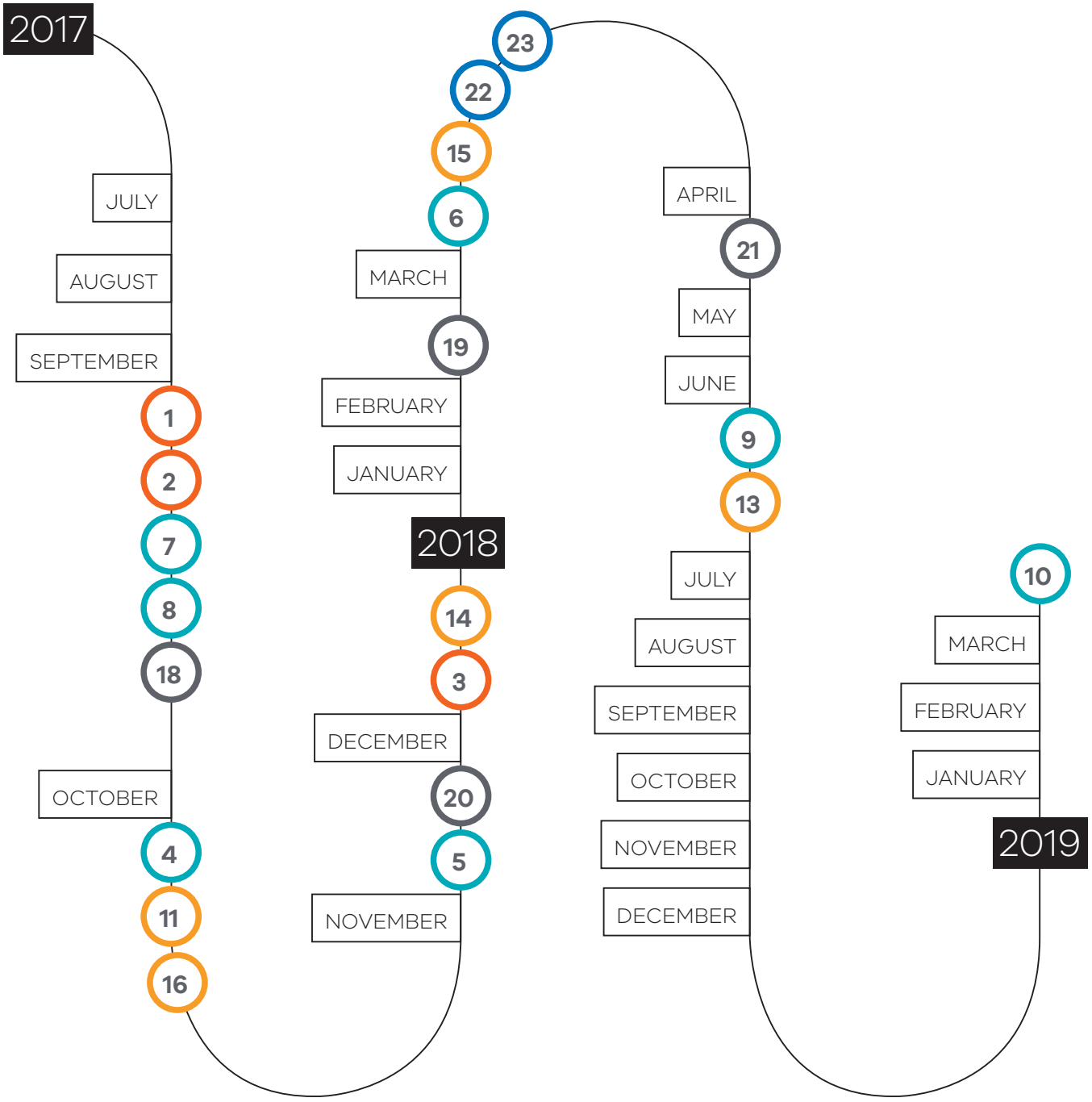
CAPABILITY

ACTION		DUE
22	Commence implementation of the cyber security capability recommendations released as part of the IT Capability Uplift Plan and developed under the *Victorian Government IT Strategy*	**March 2018**
23	Develop a workforce plan to attract, develop and retain specialist cyber security skills	**March 2018**

SCOPE

To deliver confidence in Victorian Government ICT, and support new government digital service delivery initiatives, this strategy will apply to the whole of the Victorian public service.

TIMELINE



ACTIONS

- ENGAGEMENT
- PARTNERING
- PLANNING
- SERVICE MATURITY
- CAPABILITY

CYBER SECURITY STRATEGY GROUP

This Strategy was developed under the guidance of the following expert committee. The Victorian Government extends its thanks, and acknowledges their contribution.

Geoff Beggs (Chair)	Director, Government ICT Strategy and Policy, Department of Premier & Cabinet
Jack Blayney	Assistant Commissioner and Chief Information Officer, Victoria Police
Mike Burgess	(former) Chief Information Security Officer, Telstra
Ben Heyes	Chief Information Security & Trust Officer, Commonwealth Bank of Australia
Steve Hodgkinson	Chief Information Officer, Department of Health and Human Services
Berin Lautenbach	Acting Chief Information Security Officer, Telstra
Loris Meadows	Director of Information Management and Assurance, Victoria Police
Sandra Ragg	Assistant Secretary, Cyber Policy, Department of Prime Minister & Cabinet
Michael Scotton	Assistant Secretary, Cyber Security, Australian Cyber Security Centre
Daniel Muchow	Manager, Cyber Outreach, Commonwealth Bank of Australia
Rob Heselev	Senior Executive Partner, Gartner
Shaun Steinfort	Advisor, Gartner
Jeff Warren	Cyber Security Advisor, Department of Premier & Cabinet

Victorian Government Information Technology Strategy 2016-2020: 2017-18 Action Plan

CONTENT COORDINATION

Editorial services by Department of Premier and Cabinet, Enterprise Solutions

Design by Claire Ho Design

All images by iStock

PRINT PRODUCTION

Printed by Finsbury Green, Melbourne

ACCESSIBILITY

If you would like to receive this publication in an accessible format, please contact the department on 9651 5111

Information in this document is available on **enterprisesolutions.vic.gov.au**

This report is printed on Maine Recycled – Silk, from K.W.Doggett Fine Paper. Cover pages 300 gsm and internal pages 150 gsm. Maine Recycled – Silk is carbon neutral certified and features 60% certified post consumer waste-recycled and 40% certified virgin fibre sourced from responsibly managed forests.

ISBN 978-1-925551-64-8 (pdf/online)

Authorised and published by the Victorian Government
1 Treasury Place, Melbourne 3002


VICTORIA