NSW Government
Cyber Security Strategy

A cyber safe NSW:
Connected, protected and trusted

NSW GOVERNMENT

CONTENTS

Minister’s foreword

In the 21st century, we live in a world where virtually every aspect of our life has been enhanced by digital technologies. Whether you are at home, in the workplace, or out with friends, chances are there is an app on your phone, computer, or even fridge that seeks to improve your experience.

To bring about this revolution, industries from around the world have transformed their business models, investing heavily in information technology. Similarly, in line with the Digital Government Strategy[1], the NSW Government is working tirelessly to harness digital technologies to help streamline its services and operations. We see digital transformation as a means of optimising the use of public resources and enabling our government to focus on the citizen experience.

Notwithstanding the tremendous benefits brought by the digital era, we must also address growing risks. Advanced malicious cyber activity against Australian national and economic interests is increasing in frequency, scale, sophistication and severity[2]. With this in mind, the **NSW Cyber Security Strategy** has been developed to guide and inform the safe management of government’s growing cyber footprint.

The Strategy outlines a risk-based approach that will play an important role in safeguarding citizen data and critical government services. Importantly, the Strategy is supported by $20 million in government funding which will allow for the effective delivery of its initiatives.

This Strategy takes its place alongside Australia’s Cyber Security Strategy[3] and the NSW Cyber Security Industry Development Strategy driven by the NSW Department of Industry[4].

Developing strong cyber capabilities that scale with our ambitious digital agenda, will be key to our success. By investing in cyber security today, we are enabling the NSW Government to accelerate digital transformation while providing confidence to citizens who trust us with their data and services.

The Hon. Victor Dominello, Minister for Finance, Services and Property

[1] **www.digital.nsw.gov.au**

[2] Australian Cyber Security Centre 2017 Threat Report **www.acsc.gov.au/publications/ACSC_Threat_ Report_2017.pdf**

[3] Australia’s Cyber Security Strategy: Enabling innovation, growth and prosperity **https://cybersecuritystrategy.pmc.gov.au/**

[4] In development.

> “Effective cyber security, robust risk controls and strong information management are central to maintaining the confidence and trust of our customers. From individual transactions to critical information sharing across agencies, a strong framework for managing information security and cyber risks is a pre-requisite for any modern digital government.”

NSW Digital Government Strategy

The cyber security imperative

An **integrated** approach to **preventing** and **responding** to **cyber security threats** across NSW **safeguarding** our **information, assets, services** and **citizens**

secure • integrated • responsive • holistic

Definition

Cyber security: actions required to preclude unauthorised use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets[5].

Focus on risk

As the NSW Government leads the way on streamlined digital service delivery, we must also increase cyber resilience and invest to protect against cyber threats. A priority remains to reduce the impact of cyber attacks which may have a cascading effect on the lives of citizens and the functioning of our critical infrastructure.

Recent years have seen a deterioration in the global cyber security environment with a notable increase in political hacktivism, espionage, sabotage, and financially driven cyber crime. The Australian Cyber Security Centre (ACSC) has identified an increase in diverse and innovative attempts to compromise government networks, along with foreign states increasing their level of investment in offensive cyber capabilities[6].

The ransomware criminal economy grew by more than 2,500 per cent between 2016 and 2017[7]. There are predictions that cyber crime damages will cost the world $6 trillion annually by 2021 from $3 trillion in 2015[8]. Global ransomware damage costs are predicted to climb from $5 billion in 2017 to $11.5 billion in 2019[9]. Cyber attacks increasingly exploit human vulnerabilities and organisational failings rather than purely gaps in security technology.

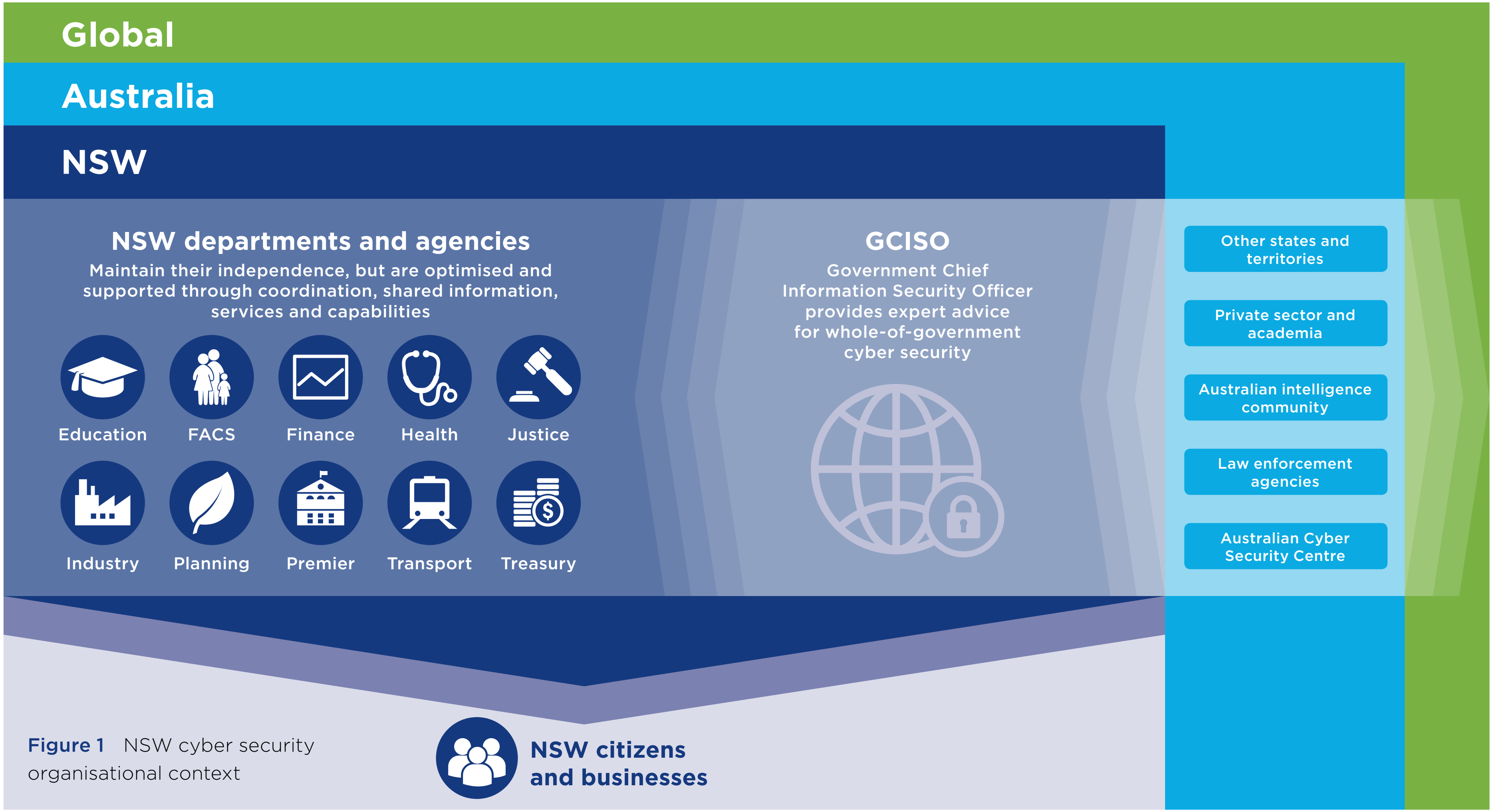
In 2017, the first NSW Government Chief Information Security Officer (GCISO) was appointed to build whole-of-government cyber security capabilities and standards. Since being established, the GCISO has laid the foundations for the whole-of-government cyber security practice, providing basic coordination and support for agencies and a single point-of-contact for the receipt and sharing of cyber security information across NSW Government.

The Cyber Security Senior Officers Group (CSSOG) has been established to provide for whole-of-government decision-making for cyber security. Members represent the key business owners of cyber risk from across NSW Government. The group's focus is on supporting the GCISO in minimising the impact of cyber risk to NSW (citizens, business and government agencies) and integrating cyber risk into the emergency management and counter terrorism frameworks.

[5] International Standard: IEC/TS 62443-1-1 ed. 1.0
[6] Australian Cyber Security Centre 2017 Threat Report **www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf**
[7] The Ransomware Economy (October 2017): Carbon Black Report **www.carbonblack.com/wp-content/uploads/2017/10/Carbon-Black-Ransomware-Economy-Report-101117.pdf**
[8] **www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html**
[9] **https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/**

Cyber security in NSW Government context

Cyber security is a global concern and requires engagement across jurisdictions and sectors including Commonwealth, State and Territory Governments, industry and research organisations.



Global

Australia

NSW

NSW departments and agencies

Maintain their independence, but are optimised and supported through coordination, shared information, services and capabilities

GCISO

Government Chief Information Security Officer provides expert advice for whole-of-government cyber security

- Other states and territories
- Private sector and academia
- Australian intelligence community
- Law enforcement agencies
- Australian Cyber Security Centre

NSW citizens and businesses

Figure 1 NSW cyber security organisational context

Principles of cyber security in NSW Government

Secure
Government systems are secure and resilient to evolving cyber incidents. Non-negotiable minimum security standards are applied across the sector. Our approach is risk-based with an emphasis on securing high impact information and services.

Integrated
Agencies coordinate and collaborate with other agencies, jurisdictions and the private sector within a federated framework, acknowledging that they are interdependent and cannot operate in isolation. Security is not an afterthought, but is integrated into all ICT assurance processes to ensure that our systems are secure-by-design.

Responsive
Agency capability is lifted through collaboration, training and support. Strong and agile teams are embedded across the sector to ensure timely response to cyber threats and incidents.

Holistic
Our technical and human capabilities are interconnected and interdependent. From a cyber risk perspective, they operate as one system. We have a ‘joined-up’ mindset, recognising that everyone takes responsibility for cyber security. This requires deep collaborative relationships across sectors and jurisdictions.

The NSW Cyber Security Strategy now sets the course for achieving this commitment.

Purpose

The NSW Digital Government Strategy articulates an ambitious plan that will transform life in NSW through smart, simple and seamless services. Ensuring a cyber safe NSW is critical to realising this plan. The NSW Cyber Security Strategy is targeted at meeting the needs of government, business and citizens for connected, protected and trusted services and infrastructure.

Government

Digital services and information holdings must be secured and protected from cyber criminals who are constantly trying to circumvent our cyber security controls.

Departments and Agencies

Must trust the integrity of the whole government network, working together with confidence that their systems and data remain secure in an increasingly interconnected environment.

Businesses

Need assurance that the data they entrust to government will be protected and used appropriately. They also rely on critical services and infrastructure which government must ensure are secure and highly available.

Citizens

Provide sensitive and personal information to government. This information must be protected. They also depend upon critical services. These services must be secure, trusted and highly available.

NSW Government cyber security framework

Our framework provides themes and actions for realising the vision of a cyber safe NSW. The framework draws on the National Institute of Standards and Technology (NIST) Framework[10] which consists of standards, guidelines, and best practices to manage cyber security-related risk. Each theme within the framework is supported by actions which will deliver continual improvement across the whole of NSW Government.

Lead

Cooperation and communication across agencies and jurisdictions, nationally and internationally, and across public and private sectors to effectively meet the challenge of an interconnected and global cyber environment.

Prepare

A cyber aware culture based on a risk management approach.

Prevent

Processes, controls and well-trained staff are in place to reduce the likelihood and harm of cyber disruption.

Detect

Effective, up-to-date monitoring technology and threat intelligence, alert and advice sharing.

Respond

Clear protocols, roles, responsibilities and regular practice ensure efficient and effective action in the event of a cyber incident.

Recover

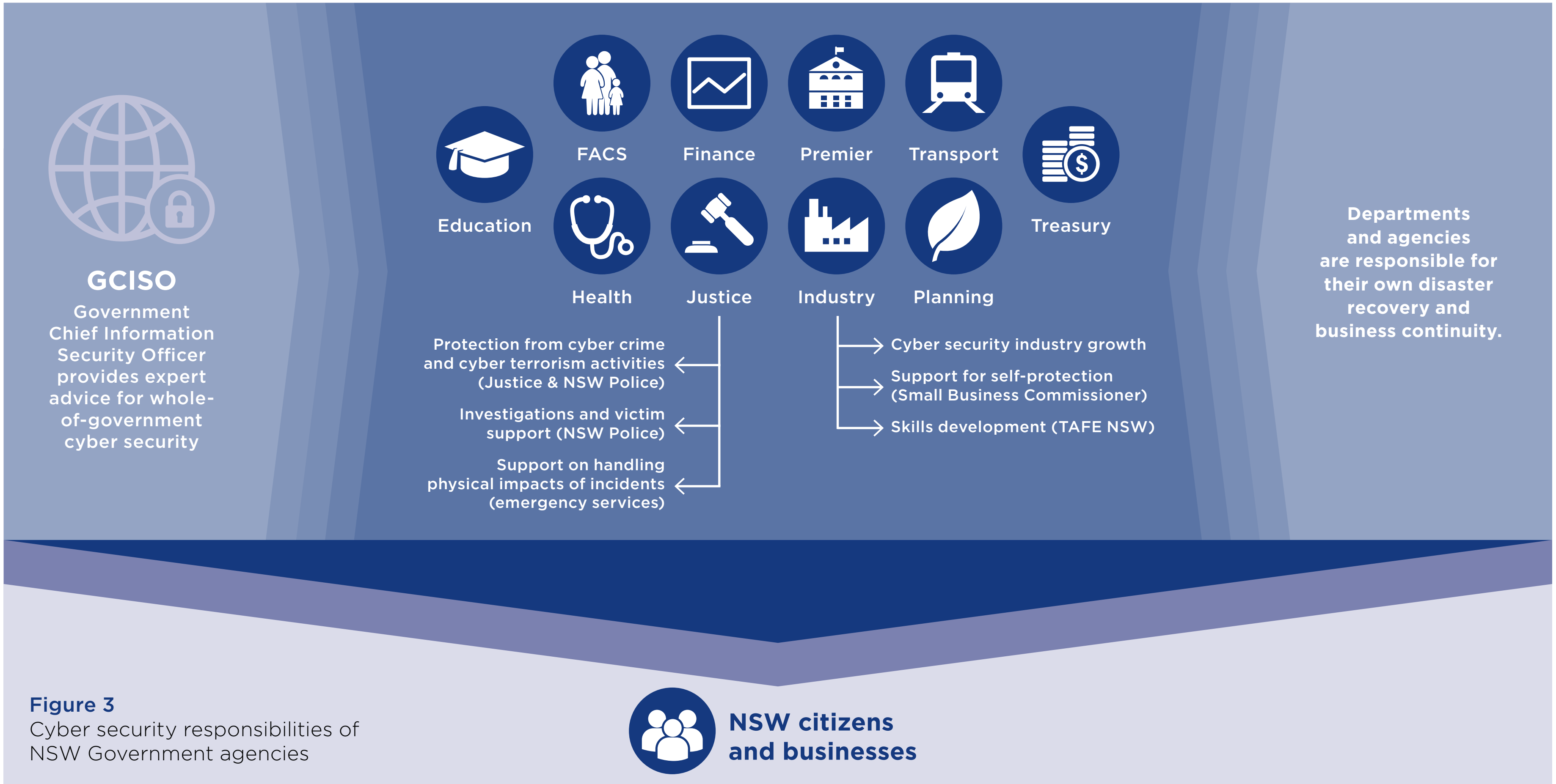
When a cyber attack causes disruption, the extent, harm and duration are minimised and government returns rapidly to business as usual.

Figure 2 NSW cyber security framework

[10] **www.nist.gov/cyberframework**

Responsibilities of NSW Government agencies

NSW Government agencies all have a role to play in ensuring a cyber safe NSW. Individual agencies are responsible for maintaining security of their own systems, services and infrastructure. The GCISO provides coordination, advice and threat intelligence. Law enforcement agencies conduct investigations and provide victim support. NSW Department of Industry and TAFE NSW provide industry and skills development.



GCISO

Government Chief Information Security Officer provides expert advice for whole-of-government cyber security

Protection from cyber crime and cyber terrorism activities (Justice & NSW Police)

Investigations and victim support (NSW Police)

Support on handling physical impacts of incidents (emergency services)

Cyber security industry growth

Support for self-protection (Small Business Commissioner)

Skills development (TAFE NSW)

Departments and agencies are responsible for their own disaster recovery and business continuity.

NSW citizens and businesses

Figure 3
Cyber security responsibilities of NSW Government agencies

Collaboration with partners and stakeholders

Effective, holistic cyber security is achieved through a strong sense of mutual responsibility between government, business, industry, researchers and the public. If each is empowered and able to fulfil its role, the security of the entire community is enhanced. Accordingly, the GCISO is working across NSW Government agencies to lift cyber security capability in the public sector.

NSW Government

NSW law enforcement and emergency response

Coordination between the GCISO, NSW police force and the State Emergency Operations Centre (SEOC) will be essential for an effective response to a serious cyber security incident, particularly if there is an impact on critical infrastructure. Similarly, the State Counter Terrorism Committee (SCTC), which coordinates terrorism-related policy, and the State Emergency Management Committee (SEMC), which provides crisis response capabilities, will work closely with the GCISO.

Infrastructure NSW

The GCISO is collaborating with Infrastructure NSW in accordance with the State Infrastructure Strategy to ensure Internet of Things (IoT) devices have cyber security risk assessments built in as part of a comprehensive assurance process.

A secure by-design approach for new infrastructure initiatives and developments will be adopted in accordance with standards set by the GCISO.

NSW Department of Industry

Through a complementary Cyber Security Industry Development Strategy, NSW Government is helping to enable innovation and encourage NSW cyber security entrepreneurs and small and medium-sized enterprises to establish and grow.

Commonwealth

Australian Cyber Security Centre (ACSC)

NSW Government, through the GCISO, is connected with Commonwealth cyber threat intelligence feeds and ensures all threat and intelligence information shared by the ACSC (including CERT, the national computer emergency response team) is appropriately distributed to all relevant stakeholders within NSW.

Joint Cyber Security Centre (JCSC)

A key initiative of the Australian Government's Cyber Security Strategy, NSW Government is participating in the Joint Cyber Security Centre (JCSC) by co-locating staff from the GCISO to ensure sensitive information, including actionable cyber threat intelligence, is shared quickly between and among partners, including leading private sector organisations. Through the Sydney JCSC, a common understanding of the cyber security environment and optimal mitigation options will be achieved through sharing and analysis of incidents, threats and risks.

Collaboration with partners and stakeholders

Academia and Research

Data61

NSW Government has partnered with CSIRO's Data61, Australia's leading data innovation group, to develop solutions for the top technology challenges facing NSW Government. These include cyber security, privacy, data sharing and enhancing skills and capabilities in the public sector.

NSW Cyber Security Network

The NSW Cyber Security Network brings together leading scientists and engineers from seven of the state's universities to protect government, industry and individuals against cyberattacks. Through the network, NSW Government will identify solutions to emerging cyber security challenges, train specialist graduates and develop a skilled cyber security workforce. It will also provide industry with strategic and operational advice on cyber security threats.

Cyber Security Cooperative Research Centre (CRC)

The CRC is charged with delivering advancements that will build Australia's cyber security capability and deliver solutions to ensure the safety of Australians and Australian businesses online.

Summary of actions to date

Leadership

- The creation of new cyber security governance arrangements, principally the Cyber Security Senior Officers Group which includes key agency leadership from across NSW Government.
- Development of the NSW Cyber Security Framework to ensure a common foundation to build cyber security capability.
- The Cyber Security Advisory Council (CSAC) has been established as a permanent independent advisory group to build strategic partnerships between government and the communities of expertise which exist across the cyber security sector. The Council includes persons from outside government with expertise in the technology, people and process dimensions of cyber security.

Capability Uplift

- Establishment of GCISO real-time advisory support service to agencies to assist with business as usual cyber security and risk management.
- Implementation of email advisories and a mobile app for whole-of-government cyber security alerts.
- A review and reformulation of the Digital Information Security Policy (DISP) and development of a draft minimum cyber security standards model and mandatory reporting arrangements.
- Development of cyber awareness materials for use across government.
- Development of a draft whole-of-government cyber incident response plan.
- Conduct of cyber security incident exercises involving NSW Government agencies, other jurisdictions and private sector partners.

Partnerships

- Commitment by the Government, in February 2018, of a $2 million investment in the new NSW Cyber Security Network, a university-led network aimed at bolstering NSW's cyber security research and development capability and harnessing the state's growing cyber security industry.
- NSW Department of Industry has prepared the Cyber Security Industry Development Strategy to encourage and promote cyber security firms in NSW.

Action plan

IMPLEMENTATION: The Action Plan comprises initiatives to be delivered by a combination of the GCISO central function and departments and agencies. Implementation governance will be via the Cyber Security Steering Group, comprised of NSW Government Chief Information Security Officers (CISOs). Departments and agencies maintain accountability for their own cyber security and responsibility over their own systems, services and infrastructure.

LEAD

Cooperation and communication across agencies and jurisdictions, nationally and internationally, and across public and private sectors to effectively meet the challenge of an interconnected and global cyber environment

START (FY)	ACTIONS	SUCCESS CRITERIA
2017/18	• Support the Counter-Terrorism, Emergency Management and Community Safety Cabinet sub-committee by providing advice on cyber risks	• Cabinet and agency leaders can make informed decisions about cyber risk
	• Provide regular briefings to the Secretaries Board, State Counter-Terrorism Committee and State Emergency Management Committee	• Senior leadership are well-informed on cyber risk and engaged in effective decision-making
	• Create and support the Cyber Security Senior Officers Group for whole-of-government cyber risk governance	• All agencies' senior leadership are well-informed on cyber risk and engaged in effective decision-making
	• Establish the Cyber Security Advisory Council to provide expert advice from outside government	• NSW Government is up-to-date with cyber trends and receives best available external advice
2018/19	• Develop shared cyber security terminology[11]	• Agencies use terminology in a consistent manner. Reporting of incidents is strengthened due to consistency of terminology

[11] Auditor-General recommendation 2.2 – Report on Internal Controls and Governance 2017 ("Internal Controls")

Action plan

PREPARE

A cyber aware culture based on a risk management approach

START (FY)	ACTIONS	SUCCESS CRITERIA
2018/19	• Establish a risk-based approach to cyber security[12]	• Cyber decision-making in agencies occurs in a systematic risk-based way
	• Develop a whole-of-government risk-based framework and communicate it across agencies	• Cyber risk is integrated into agency risk frameworks
	• Develop whole-of-government risk appetite model	• A whole-of-government risk appetite model is agreed by CSSOG and every agency's senior leadership team defines and agrees to their own cyber risk appetite statement
2017/18	• Create standard cyber security role definitions	• There are clear roles and lines of accountability for managing cyber risk
	• Establish and manage enhanced relationships with Commonwealth initiatives including Joint Cyber Security Centre (JCSC) and CERT Australia[13]	• NSW Government is actively participating in and integrated with Commonwealth initiatives • NSW cyber risk is in part mitigated through a strong relationship and clear lines of accountability with the Commonwealth
2018/19	• Partner with NSW Department of Industry to develop a cyber skills pathway model for NSW Government agencies	• A strong pipeline of cyber security talent is in place for NSW Government roles

[12] State Infrastructure Strategy recommendation 33

[13] Auditor-General recommendation 5 – Performance Audit: Detecting and responding to cyber security incidents ("Cyber Security")

Action plan

PREPARE

A cyber aware culture based on a risk management approach

START (FY)	ACTIONS	SUCCESS CRITERIA
2017/18	• Design, implement and continually improve a whole-of-government cyber risk awareness program for NSW Government employees:[14]	
	– Develop cyber awareness resources	• NSW Government employees are aware of how their personal behaviour can reduce the risk of an incident occurring
	– Integrate cyber security training into induction programs	• NSW Government employees have cyber security awareness from induction and know who their CISO is in the event they need to seek advice or report on a cyber event
2018/19	– Establish web portal for training and collaboration	• NSW Government employees are receiving up-to-date information and training on cyber security regularly
2017/18	• Establish NSW Government Cyber Readiness Program comprising:	• Roles and responsibilities during incidents are understood and regularly tested
2018/19	– Response exercises for serious cyber incidents[15]	• NSW is hardened against cyber incidents including malicious attacks or accidental damage
	– A whole-of-government incident response model including connections at a national level[16]	• Professional, operational and emergency response networks are reinforced across NSW and nationally

[14] Auditor-General recommendation 2.2 – Internal Controls; Auditor-General recommendation 2 – Cyber Security
[15] Auditor-General recommendation 2 – Cyber Security
[16] Auditor-General recommendation 4 – Cyber Security

Action plan

PREVENT

Processes, controls and well-trained staff are in place to reduce the likelihood and harm of cyber disruption

START (FY)	ACTIONS	SUCCESS CRITERIA
2017/18	• Establish a panel of approved cyber security services[17]	• Agencies have streamlined access to services to assist them in improving their cyber risk profile
	• Strengthened Digital Information Security Policy[18]	• NSW information, services and assets are protected against evolving threats
2018/19	• Establish minimum cyber security standards and require agencies to regularly assess and report against them[19]	• Standards are agreed across government and reported against regularly
	• Establish standard cyber security procurement contract terms[20]	• Agencies make efficient and informed procurement choices with certainty
	• Develop fit-for-purpose cyber assurance mechanisms for ICT and infrastructure projects[21]	• Cyber risks for ICT and connected infrastructure projects are lessened
	• Introduce a secure-by-design approach for new initiatives including the Internet of Things and connected infrastructure, and integrate this into the connected infrastructure policy framework by 2020[22]	• New ICT and connected infrastructure projects are secure-by-design

[17] Auditor-General recommendation 2 – Cyber Security
[18] Auditor-General recommendation 3, 7 – Cyber Security
[19] Auditor-General recommendation 2.2 – Internal Controls
[20] Auditor-General recommendation 6 – Cyber Security
[21] State Infrastructure Strategy recommendation 34
[22] State Infrastructure Strategy recommendation 35

Action plan

DETECT

Effective, up-to-date monitoring technology and threat intelligence, alert and advice sharing

START (FY)	ACTIONS	SUCCESS CRITERIA
2018/19	• Establish best-practice guidelines for incident detection, response and reporting[23]	• All NSW Government agencies minimise risk by following best practice incident detection, response and reporting
	• Improved Information Sharing:[24]	
	– Establish inter-agency information sharing protocol	• There is shared understanding of threats across NSW Government and a coordinated response for incidents
	– Regular notifications, security advisories and incident alerts distributed to all agencies from the GCISO and linked to Commonwealth and vendor threat intelligence feeds	• All agencies have high quality intelligence and informed cyber security decision-making
	– Establish whole-of-government threat intelligence platform[25]	• Efficient and timely dissemination of threat intelligence

[23] Auditor-General recommendation 2 – Cyber Security
[24] Auditor-General recommendation 1 – Cyber Security
[25] Auditor-General recommendation 5 – Cyber Security

Action plan

RESPOND

Clear protocols, roles, responsibilities and regular practice ensure efficient and effective action in the event of a cyber incident

START (FY)	ACTIONS	SUCCESS CRITERIA
2018/19	• Establish mandatory cyber incident reporting requirements[26]	• Information about incidents in any single agency are disseminated to other agencies to reduce impact and avert harm
	• Implement Commonwealth-State response protocols[27]	• Rapid communication and minimised delays between Commonwealth and NSW in responding to cyber events
	• Design and implement protocol for engaging NSW Emergency Management during cyber crises	• Joined-up NSW Government response to serious cyber incidents
2019/20	• Establish a NSW Government Cyber Security Coordination Centre	• NSW Government has coordinated monitoring, detection, response and reporting
	• Establish cyber security incident response and remediation advisory service	• Effective response procedures are in place. Consistent information sharing and understanding between and within agencies
	• Establish a model whereby NSW Government agencies share cyber skilled personnel during a crisis or major incident	• Benefits of skill sharing for rapid incident response realised and NSW less vulnerable to skill shortages

[26] Auditor-General recommendation 3,4 – Cyber Security
[27] Auditor-General recommendation 1 – Cyber Security

Action plan

RECOVER

When a cyber attack causes disruption, the extent, harm and duration are minimised and government returns rapidly to business as usual

START (FY)	ACTIONS	SUCCESS CRITERIA
2017/18	• Establish an identity recovery service for customers of NSW Government whose identities become compromised from a cyber incident	• Agencies refer customers to recovery services in the event of their identities having been compromised
2018/19	• Conduct resilience review of NSW capacity to recover from serious cyber events	• Recovery from cyber incidents is efficient and effective and societal impact is minimised
	• Establish post-incident review protocol[28]	• A continual improvement approach is in place which ensures the lessons are documented and processes improved after incidents to lessen the likelihood and impact of the same issues reoccurring

[28] Auditor-General recommendation 1 – Cyber Security

NSW
GOVERNMENT