Submission
No 10

INQUIRY INTO CYBERSECURITY

Organisation:	NSW Government
Date Received:	17 September 2020

Cyber Security NSW Submission to Portfolio Committee No 1 (Premier and Finance) on the Inquiry into Cybersecurity

Department of Customer Service

SEPTEMBER 2020

Contents

NSW Cyber Security Strategy

Published in 2018, the *NSW Government Cyber Security Strategy*[1] outlines a risk-based approach to safeguarding citizen data and critical government services, and is aligned with the Australian Cyber Security Strategy. The Strategy is based on four NSW Government cyber security principles:

1. Secure – government systems are secure and resilient to evolving cyber incidents
2. Integrated – agencies coordinate and collaborate with other agencies, with security integrated into all ICT assurance processes with the goal for all systems to be secure by design
3. Responsive – agency capability is lifted, and teams are embedded across the sector to ensure timely responses to cyber threats and incidents
4. Holistic – that the cyber security approach and response is interconnected and integrated, with deep collaborative relationships across sectors and jurisdictions.

In July 2020, the NSW Government announced the development of an updated comprehensive, sector-wide cyber security strategy.

The 2020 Strategy will replace the *NSW Cyber Security Strategy 2018* and the *NSW Cyber Security Industry Development Strategy*[2], combining them into one overarching cyber security strategy for NSW. This recognises the connection between a strong government cyber security posture and a strong cyber security industry.

Industry partners and cyber security experts were invited to provide a submission to the 2020 Strategy for consideration by the NSW Government. Key focus areas for the new strategy include:

- cyber security resilience
- the cyber security workforce and skills gap
- helping NSW cyber security businesses grow, and
- supporting cyber security innovation and research and development.

The 2020 Strategy will be published later this year.

NSW Cyber Security Policy

In February 2019, the NSW Government released the *NSW Cyber Security Policy*[3], a risk-based policy based on the National Institute of Standards and Technology (NIST) cyber security framework.

The policy outlines the mandatory requirements to which all NSW Government departments and public service agencies must adhere, to ensure cyber security risks to their information and systems are appropriately managed.

The policy sets out the roles and responsibilities of key agency decision makers, including:

- Chief Executives
- Chief Information Officers
- Chief Information Security Officers
- Cyber Security NSW
- Chief Cyber Security Officer.

The policy sets out a number of mandatory requirements for planning and governance, cyber security culture, cyber security risks, resilience, reporting and attestation.

More specifically, the policy requires all government agencies to:

- strengthen cyber security governance
- identify their most valuable or operationally vital systems or information ("crown jewels")
- strengthen cyber security controls
- develop a cyber security culture across all staff
- work across all of government to share security and threat intelligence, and
- implement a whole of government approach to cyber incident response.

The policy is reviewed and updated during each reporting period, based on agency feedback and emerging cyber security threats.

Mandatory requirements

The policy is risk-based in nature, but outlines 25 mandatory requirements all NSW agencies must implement and report against. As a new feature of the policy, NSW was the first Australian State and Territory jurisdiction to require agencies to implement and assess maturity against the Australian Cyber Security Centre's (ACSC) Essential 8 risk mitigation controls.

Given the risk-based nature of the policy, NSW agencies report their maturity against the Essential 8 controls, but also list additional security controls that mitigate cyber risk.

The mandatory requirements, and Essential 8 controls and reporting, provide Cyber Security NSW with a whole-of-government view of agency maturity. It allows agencies to target the areas in most need of uplift. Agencies are working to uplift their cyber security and ensure vulnerabilities are addressed and remediated.

Under the policy, agencies must appoint staff to roles that cover a broad range of cyber security activities:

- key leadership positions (Secretary/Agency Head, NSW Chief Cyber Security Officer)
- key management positions (Chief Information Officer, Chief Information Cyber Security Officers, Chief Operating Officer, Information Security Manager/Cyber security Manager)

- supporting teams/positions (Information Management Officer, Internal Audit, Risk staff), and
- vendors and third Parties (vendors and consultants).

Individual clusters and agency heads, in conjunction with Chief Information and Chief Information Security Officers, are responsible for complying with the policy, implementing agency level cyber and information security plans, and maintaining an effective cyber security program.

The maturity of an agency's planning and governance arrangements is assessed each year through reporting against the policy.

Cyber Security NSW is undertaking its second year of maturity reporting and gaining a clearer understanding of NSW cyber security strengths and weaknesses.

As the remit of Cyber Security NSW expands to local councils, following recently announced cyber security stimulus funding, the policy, guidance and assistance in building capability will help ensure all government agencies, and councils, report against the policy and improve cyber security controls.

Cyber security governance arrangements

NSW cyber security is a whole-of-government concern. The ICT and Digital Leadership Group comprises senior executives from across all clusters. It considers and endorses cyber security policy, and reviews agency cyber security reports with the Cyber Security Senior Officers' Group (cyber security leaders from across government) to identify common concerns and areas for improvement.

The Secretary of the Department of Customer Service (DCS) gives effect to the policy through a whole-of-government circular which clearly sets out compliance requirements.

Cyber Security NSW, part of DCS, focuses on enhancing whole-of-government cyber security capabilities and standards, improving cyber incident response coordination and overseeing the development of strategic cyber policies. It works closely with federal agencies, including the ACSC and the Joint Cyber Security Centre (JCSC).

In the case of cyber security incidents, individual clusters and agencies are responsible for monitoring and responding to these in the first instance. Under the policy, clusters and agencies are required to report cyber security incidents to the appropriate agency governance forum (for example the Chief Information Security Officers Council or the ICT and Digital Leadership Group) and Cyber Security NSW based on their risk profile.

In addition to cross-government monitoring, Cyber Security NSW works closely with the ACSC on cyber security threats and risks given that many originate outside of Australia.

Where a criminal cyber offence may have occurred, the NSW Police Force (NSWPF) has responsibility for investigating.

Emergency management arrangements

Cyber security threats need to be managed at the whole-of-government level. As such, in 2018, the NSW Government published its first *Cyber Security Incident Emergency Sub Plan*[4]. This Sub Plan sits under *State Emergency Management Plan* (EMPLAN) and is the whole-of-government plan for significant cyber security incidents or crises affecting NSW Government organisations.

The *Cyber Security Incident Emergency Sub Plan* aims to protect the NSW community from potential consequences of a significant cyber security incident or crisis. It outlines the interaction between the cyber security community, business continuity personnel and the emergency management sector to reduce impacts to NSW Government services, assets and infrastructure, coordinate information flow between agencies, and communicate to the public in relation to these events.

NSW Government agencies are responsible for the operational response to any incident affecting NSW Government systems or services. In the event of a cyber incident, the Sub Plan outlines the responsibilities for the following roles:

- Emergency Cyber Security Operations Coordinator – in the event of a significant cyber security incident or crisis, the NSW Chief Cyber Security Officer assumes this role, which undertakes a broad range of roles in support of the Senior Officers' Group and the State Emergency Operations Controller.
- State Emergency Operations Controller – in the absence of a prescribed response agency, this role takes responsibility for the control and coordination of management of the incident.
- Senior Officers Group is responsible for activating cluster and agency business continuity plans to take required response actions, briefing their respective cluster Secretaries/Ministers on the actions and broader communications.
- Technical Officers Group – is responsible for forming a whole of government view of the scale and nature of the cyber incident in terms of its impacts and duration. It is chaired by the Director of Cyber Security Operations (who reports to the Chief Cyber Security Officer).
- Public information and the Communications Group – provides information and communications on the cyber crisis.
- The Department of Customer Service and the Department of Premier and Cabinet represent NSW on the National Crisis Committee, with DCS leading the NSW response to impacts on NSW Government digital assets.

Figure 1 outlines the current responsibility and communication arrangements during a significant cyber incident.

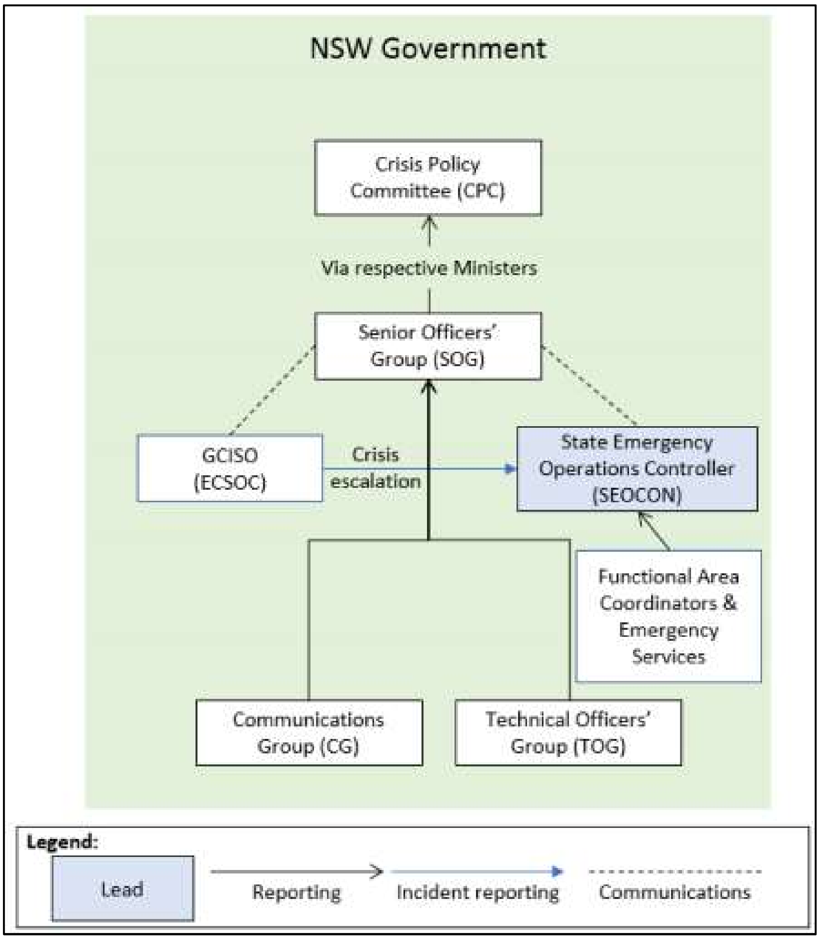
NSW Government
Crisis Policy Committee (CPC)
Via respective Ministers
Senior Officers' Group (SOG)
GCISO (ECSOC)
Crisis escalation
State Emergency Operations Controller (SEOCON)
Functional Area Coordinators & Emergency Services
Communications Group (CG)
Technical Officers' Group (TOG)
Legend:
Lead
Reporting
Incident reporting
Communications

Figure 1: NSW Cyber Crisis Response Process

Future cyber security capability

$240 million investment

On 18 June 2020, the NSW Government announced a critical investment of $240 million over 3 years for state-wide cyber security maturity uplift across the NSW Government, administered through the Digital Restart Fund.

This includes an investment of $60 million to expand the remit of Cyber Security NSW to smaller government agencies and councils, and will allow the branch to undertake a proactive approach to cyber threat management and response.

The remaining $180 million of the $240 million cyber security allocation will be invested in clusters for targeted cyber security uplift to better manage and address cyber security risks, improve the maturity of cyber security practice in agencies as they implement technical safeguards, and align to best practice standards in the Cyber Security Policy.

Implementation of DMARC

In 2018, the NSW Government commenced implementation of a Domain-based Messaging, Authentication, Reporting and Conformance (DMARC) and government brand protection solution. This project is crucial to protecting NSW Government customers. Working with cyber security teams in all clusters, the project is focused on making it harder for cyber criminals to send fake emails and impersonate NSW Government websites.

Establishment of the Vulnerability Management Centre

Early detection of vulnerabilities and the ability to report them to the relevant agencies and departments is essential to improving our cyber security. Launched in June 2020, the *NSW Vulnerability Management Centre* in Bathurst will deliver vital, sector-wide risk management capability and is critical to ensuring enhanced monitoring of at-risk government systems, and early identification and remediation of known vulnerabilities.

The Centre became operational in July 2020 and is a significant boost to regional development and employment. It is an example of the NSW Government's commitment to investing in regional NSW, creating jobs and keeping money in local economies. As the Centre expands, it will bring skilled workers to the region to further promote cyber employment opportunities in regional NSW.

Harmonisation of cyber security standards

In June 2020, the Minister for Customer Service announced the creation of the *Standards Harmonisation Taskforce*. The taskforce will harmonise baseline cyber security standards and clarify additional sector-specific standards and guidance. It is a collaboration between NSW Government, AustCyber and Standards Australia.

In addition, the taskforce aims to enhance competitiveness standards in the cyber sector for suppliers and consumers and support Australian cyber security companies to seize opportunities globally.

Working with local councils

Cyber Security NSW is engaging with a number of local councils to provide cyber security support with tailored workshops, resources and training sessions. Members from 42 different councils have registered for the Cyber Security NSW Essentials Training with over 600 staff from these local councils registered.

Cyber Security NSW is working with the Office of Local Government to support councils with cyber security policies and guidance.

Contractual requirements and procurement

The *Procurement Policy Framework*[5] applies to the procurement of goods and services of any kind, including construction.

Procurement Board Direction 2020-02[6] mandates use of the *Procure IT Framework* by NSW Government agencies when procuring ICT and digital services and infrastructure.

The *Procure IT Framework* comprises:

- *Procure IT v3.2*[7] – for all ICT procurement over $1,000,000 and all high-risk ICT procurement from 1 September 2017
- *Core& Contracts (Low Risk)*[8] – for all low risk ICT procurement up to the value of $1,000,000 (excluding GST) from 1 November 2018

Both forms of agreement have provisions relating to cybersecurity.

At a whole-of-government level, the *Procure IT Framework* is administered by DCS. This framework has been designed to provide a series of protections for NSW Government agencies.

The contract templates have included requirements for managing customer data, security, data breach, privacy, audit and reporting. Relevant provisions are:

- In *Procure IT v3.2*, the high-risk template, clauses 7.1 – 7.12 relate to security, clause 15 relates to privacy and clauses 23.4 – 23.11 relate to audit and contract administration. In *Core& Contracts*, the low-risk template, clause 9 deals with security obligations.
- In *Procure IT v3.2*, clause 21.1 relates to contractual reporting obligations. In *Core& Contracts*, clause 11 relates to monitoring.

The contracting framework includes clauses relating to source code/escrow deeds, location of data and cross border transfer of data.

In accordance with *Procurement Board Direction 2020-02*, agencies must also complete a risk assessment to ensure the appropriate use of Procure IT framework contracts.

Agencies are accountable for managing risks and ensuring each contract complies with mandatory policies including the *NSW Government Cyber Security Policy*. However, DCS manages a robust governance process of variations to the *Procure IT Framework*. DCS ensures agencies' submissions address the adequacy of proposed terms and management of associated risks.

The existing contracting framework provides an adequate commercially focused and balanced structure in addressing source code, data flow and data location issues in addition to protections for managing customer data, security, data breach, privacy, audit and reporting.

For example, under the *Procure IT Framework*, cross-border transfers of data require the consent of the government agency. If consent is granted, the relevant agency must specify within the *Procure IT* agreement the jurisdictions for which consent is granted, and the conditions on which such consent is granted.

DCS offers guidelines and support to allow agencies to have an effective risk management for ICT procurement including templates, guides, questionnaires and checklists, all of which are publicly available on the *buy.nsw* website.

Whole-of-government data centre arrangements

Whole-of-government circular *DFSI-2018-02 – Data Centre Reform*[9] requires agencies to relocate remaining data centre and computer room infrastructure from current (on premise and leased) facilities into the Government Data Centres (GovDC) and, where appropriate, consume services through the GovDC Marketplace or other suitable cloud services.

The GovDC locations are Tier III certified, 100% uptime, vendor neutral, highly secure, ISO27001 certified. GovDC has been designed and built to a high level of physical security. Some of the security features are:

- 6 physical security zones
- 24-hour onsite guards
- 3-metre-high anti-scale fences
- PAS68 hostile vehicle barriers.
- Over 150 security cameras per site

Agency tenants are responsible for the management of their systems within GovDC. This includes management of outages, backups and cyber security.

Other key policies relating to cyber security

Key whole of government policies support management of digital information, including:

- *NSW Government Cloud Policy*[10] – provides practical steps to move services to cloud. The policy is accompanied by Guidelines for consumption of cloud services.
- *NSW Smart Infrastructure Policy*[11] – requires consideration of security (including data security) and implementation of privacy by design for new smart infrastructure.
- *NSW Government Internet of Things (IoT) Policy*[12] – includes data management, security and privacy advice for agencies using IoT enabled devices and equipment.
- *NSW Government Artificial Intelligence Strategy and Ethics Policy*[13] – includes privacy by design and cyber security requirements.
- *NSW Information Management Framework*[14] – a practical tool that outlines the direction for information and data management in the NSW Public Sector, with a focus on security, risk and compliance assessments.
- *NSW Information Classification, Handling and Labelling Guidelines*[15] – assist agencies to correctly assess the sensitivity of information, so that information that is sensitive in nature is correctly labelled, used, handled and stored appropriately.

[1] *NSW Government Cyber Security Strategy (2018)* – https://www.digital.nsw.gov.au/sites/default/files/NSW%20Cyber%20Security%20Strategy%202018.pdf

[2] *NSW Cyber Security Industry Development Strategy (2018)* – https://www.business.nsw.gov.au/industry-sectors/industry-opportunities/cyber-security

[3] *NSW Government Cyber Security Policy* – https://www.digital.nsw.gov.au/policy/cyber-security-policy

[4] *NSW Cyber Security Incident Emergency Sub Plan* – https://www.emergency.nsw.gov.au/Pages/publications/plans/sub-plans/cyber-security.aspx

[5] *Procurement Policy Framework* – https://buy.nsw.gov.au/policy-library/policies/procurement-policy-framework

[6] *Procurement Board Direction 2020-02: Use of Procure IT Framework and increase of the threshold in Core& Contracts* – https://buy.nsw.gov.au/policy-library/procurement-board-directions/pbd-2020-02-use-of-procure-it-framework-and-increase-of-the-threshold-in-core-and-contracts

[7] *Procure IT 3.2* – https://buy.nsw.gov.au/resources/procure-it-v3.2

[8] *Core& Contracts* – https://buy.nsw.gov.au/resources/core-and-contracts

[9] *DFSI-2018-02 Data Centre Reform* – https://arp.nsw.gov.au/dfsi-2018-02-data-centre-reform

[10] *NSW Government Cloud Policy (2018)* – https://www.digital.nsw.gov.au/policy/buying-ict/cloud-guidance-and-policy

[11] *NSW Smart Infrastructure Policy* – https://www.digital.nsw.gov.au/policy/smart-infrastructure-policy

[12] *NSW Internet of Things (IoT) Policy* – https://www.digital.nsw.gov.au/policy/internet-things-iot

[13] *NSW Artificial Intelligence Strategy and Ethics Policy* – https://www.digital.nsw.gov.au/policy/artificial-intelligence-ai

[14] *NSW Information Management Framework* – https://data.nsw.gov.au/information-management-framework

[15] *NSW Information Classification, Handling and Labelling Guidelines* – https://data.nsw.gov.au/information-classification-handling-and-labelling-guidelines