NSW Cyber Security Incident Emergency Sub Plan

A Sub Plan of the *State Emergency Management Plan*

Endorsed by the State Emergency Management Committee

December 2018

NSW emergency management plans are updated regularly and accordingly printed plans may be out of date.

The current plan is always available at
www.emergency.nsw.gov.au

Authorisation

The Cyber Security Incident Emergency Sub Plan is a Sub Plan to the State Emergency Management Plan (EMPLAN) to detail the procedures and coordination arrangements for the NSW Government in prevention of, preparation for, response to, and initial recovery from, an emergency that is the consequence of a significant cyber security incident or a cyber security crisis affecting NSW Government organisations.

This Sub Plan is endorsed by the State Emergency Management Committee in accordance with the provisions of the *State Emergency and Rescue Management Act 1989* (NSW).

Endorsed by the State Emergency Management Committee
December 2018
SEMC Meeting 111

VERSION CONTROL

Proposals for amendments to content of this Sub Plan are to be forwarded to:

NSW GCISO
cybersecurity@finance.nsw.gov.au

VERSION HISTORY

Version	Date
0.1	September 2018
1.0 Initial Issue	December 2018

DISTRIBUTION

This Sub Plan is not distributed in hard copy. Organisations and individuals should confirm they have the latest copy by checking the current version at www.emergency.nsw.gov.au.

Contents

1 Introduction

General

1.1 The *New South Wales (NSW) Cyber Security Incident Emergency Sub Plan* is a Sub Plan to the State Emergency Management Plan (EMPLAN). This plan does not require activation as the arrangements it describes are always 'active'. It can operate concurrently with other plans.

Purpose

1.2 The *NSW Cyber Security Incident Emergency Sub Plan* is the whole-of-government plan for significant cyber security incidents or crises affecting NSW Government organisations.

1.3 This plan outlines the strategic intent, procedures and coordination arrangements for the NSW Government in prevention of, preparation for, response to, and initial recovery from a significant cyber security incident or crisis.

1.4 This plan aims to protect the NSW Community from potential consequences of a significant cyber security incident or crisis. It describes 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.

Background

1.5 Cyber security is defined as "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"[1].

1.6 There is an accelerating deterioration in the global cyber security environment with a notable increase in political and geopolitical hacktivism, espionage, industrial sabotage, and financially-driven cybercrime. Cyber security incidents are now a normal event rather than a remote possibility, with insurers approaching cyber risk in the equivalent manner to natural disaster risk. The insurance firm Lloyd's reports a major global cyberattack has the potential to trigger up to $53 billion of economic losses, roughly the equivalent to a catastrophic natural disaster.[2]

1.7 The ransomware criminal economy grew by more than 2,500% in 2017. Two significant global incidents occurred in mid-2017. WannaCry resulted in chaos for the UK National Health Service including 19,000 surgery cancellations, and impacted approximately 400,000 devices worldwide.[3] Thirty-four percent of Hospital an Primary Care Services were shut down or impacted over six

[1] International Standard: IECT/TS 62443-1-1 ed. 1.0

[2] https://www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report

[3] https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/

days. Subsequently, the Petya virus impacted hundreds of organisations globally. NSW Government was fortunate not to be impacted by these incidents but cannot expect to be immune in future.

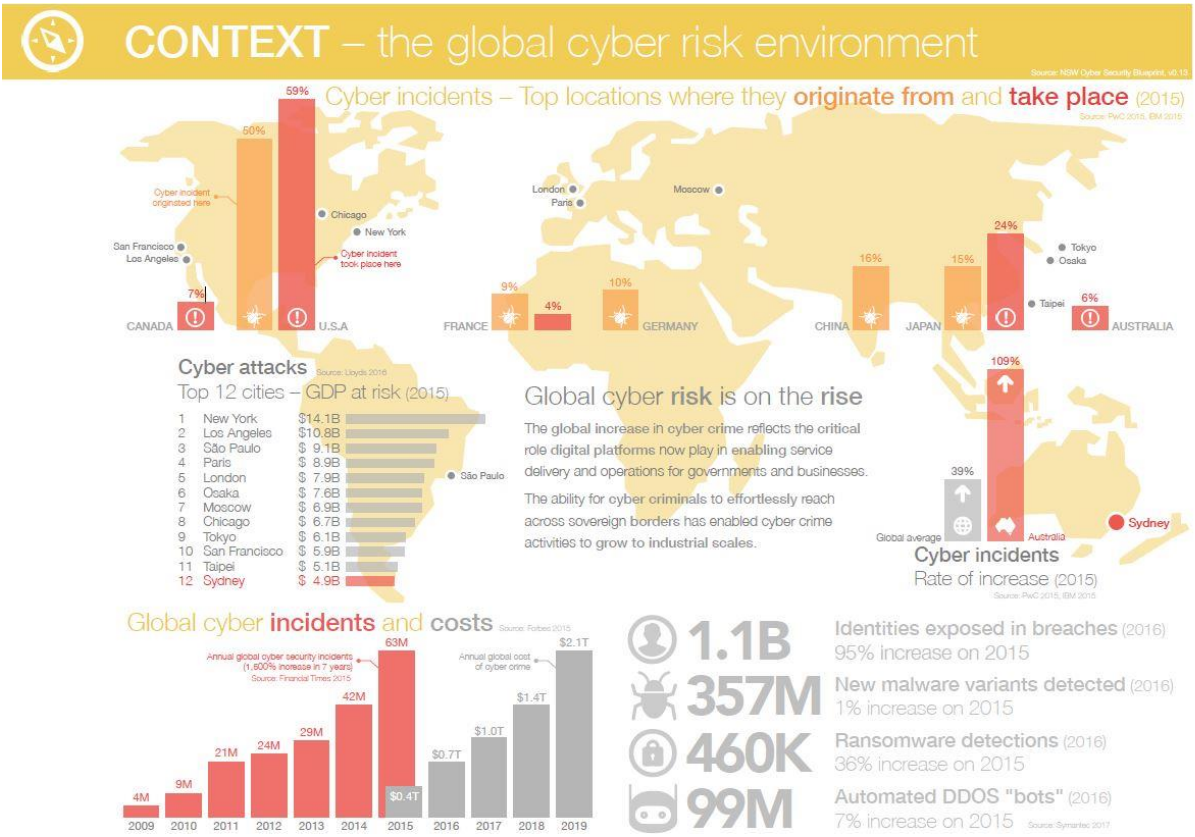

Figure 1: Global Cyber Risk Environment

1.8 There are predictions that cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. As a type of crime, this will be more profitable than the global trade of all major illegal drugs combined.[4]

1.9 The global increase in cybercrime parallels the progressively critical role digital platforms play in enabling service delivery and operations for governments and businesses.

1.10 As recognised by the NSW Digital Government Strategy (2017), robust cyber security is essential for maintaining the confidence and trust of customers. As the NSW Government leads the way on streamlined digital service delivery, we also increase cyber dependency. Government must take all reasonable precautions to ensure the continuity and performance of essential government

[4] https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

services.

Scope

1.11 The *NSW Cyber Incident Emergency Sub Plan* describes the roles and responsibilities of the Government cyber security community, NSW Government agencies and the emergency management sector in the event that a cyber security incident results in a threat to people, property or the environment in NSW.

1.12 This plan details arrangements that are additional or different to those in the NSW State Emergency Management Plan (EMPLAN) and should be read in conjunction with the EMPLAN and its subordinate arrangements. This plan can operate concurrently with other plans.

1.13 This plan does not apply to the coordination of the NSW Government response to a cyber security incident that does not result in an 'emergency' as defined by the *State Emergency and Rescue Management Act 1989*. The NSW Government Chief Information Security Officer maintains the *NSW Cyber Incident Response Plan*, which describes the specific response to such cyber incidents.

1.14 The Government Chief Information Security Officer (GCISO) may be required to provide subject matter expertise to NSW Government and coordinate with the private sector in instances where there is a significant cyber security incident or cyber security crisis affecting private sector or non-government organisations.

NSW Cyber Security Incident Response Plan

1.15 The NSW Cyber Security Incident Response Plan (Response Plan) describes the response to a cyber security incident regardless of whether or not the broader consequences constitute an emergency. The Response Plan sets out the process for coordination across multiple cyber security stakeholders including NSW Government clusters, local councils, other jurisdictions, the Commonwealth and the private sector.

1.16 The Response Plan and this Sub Plan operate in parallel. These plans are not hierarchical however if a conflict arises the protection of human life and the environment takes priority above all other obligations.

1.17 Classification of cyber incidents is guided by the *NSW Cyber Incident Response Plan*. Classification decisions are made by the GCISO who informs the State Emergency Operations Controller (SEOCON) of the plans and actions being undertaken in response to the cyber incident. (See Section: Response)

1.18 **A significant cyber security incident** means an incident or series of incidents having cumulative effects which involves impact on multiple NSW Government agencies resulting in either:

- impact on reputation of NSW Government and/or government services
- disruption to activities of NSW business and/or the community

1.19 Key indicators of a significant cyber security incident include:

- causing NSW Government service impacts and driving heightened media interest
- having impact beyond a single target government organisation requiring broader NSW

Government action and communication

1.20 **A cyber security crisis** means an incident or series of incidents having cumulative effects which involves impact on multiple NSW Government agencies resulting in:

- major disruptions to NSW Government services and operations, with risks to critical infrastructure and services, to businesses, or to the safety of the public

1.21 Key indicators of a cyber security crisis include:

- Real-world impacts requiring emergency management interventions and threats to essential services and critical infrastructure
- Possibly concurrent series of incidents and spanning multiple jurisdictions
- Potential whole of government, national, global and community impacts

2 Prevention

2.1 An important component of the NSW Digital Government Strategy is the strengthening of NSW Government's ability to protect itself against cyber threats. Citizens and businesses need to be confident that the data entrusted to government and the digital services they use are secure, resilient and reliable.

2.2 Appropriately managing cyber security is fundamentally important to the reputation of the NSW Government, and to citizens' trust in government. All NSW public service agencies therefore have significant responsibilities for managing cyber and information security risks.

2.3 It has been identified, and real-world experience demonstrates that societies' reliance on computer networks means cyber security incidents can have significant real-world consequences that can cause a threat to life and property.

2.4 The current Digital Information Security Policy (DISP) adopts a risk management approach to information security so that information created and held by the Government is appropriately protected and handled. The Policy establishes:

- minimum controls
- a community of practice
- senior responsible officers (SROs) within each agency who are responsible for information security
- annual attestation and reporting requirements on security management.

2.5 In the revised Policy commencing in 2018 each of the following parties has specific assigned roles and responsibilities under the NSW Government Cyber Security Policy. Responsibilities include but are not limited to:

- Agency/Department heads -
    - Ensuring their organisation implements and maintains an effective cyber security program.
    - Attesting to the adequacy of their organisation's cyber security program in the organisation's annual report.
    - Appropriately resourcing and supporting organisational cyber security activities and responsibilities.
    - For cluster Secretaries, supporting agencies in their cluster to implement and maintain an effective cyber security program.
- NSW Government Chief Information Security Officer (GCISO) -
    - Receiving, collating and reporting on cyber risk such as incident reports, compliance with standards or maturity assessments from public service agencies.
    - Chairing the NSW Government Cyber Security Steering Group (CSSG).
    - Providing advice and assistance to the NSW Government on cyber security

including improvements to capability and capacity.

- Executive managers -
    - Ensuring they are familiar with the cyber security policies and procedures in their organisation that all staff, including consultants, contractors and outsourced service providers understand the cyber security requirements of their roles.
    - Ensuring all necessary cyber incidents are reported to the organisation's Chief Information Security Officer (CISO).
    - Coordinating the assessment and management of cyber risks to organisational assets.
    - Cooperating with their organisational CISO, Chief Information Officer (CIO), and security officers in the implementation and operation of their agency's cyber security strategy and approaches.
    - Cooperating and assisting their organisational CISO, CIO and security officers in the investigation, co-ordination and response to cyber security incidents.
- Chief Information Officers (CIOs), or key staff with information responsibilities -
    - Ensuring that all staff, including consultants, contractors and outsourced service providers, comply with this policy.
    - Ensuring all government information assets are created and managed appropriately, to ensure their effective use, control and security.
- Chief Information Security Officers (CISOs), or key staff with security responsibilities -
    - Investigating, responding and reporting on cyber security incidents.
    - Reporting relevant cyber incidents to their Agency/Department head and the GCISO.
    - Reporting on the organisation's maturity levels or adherence to relevant frameworks or standards related to this policy.
    - Establishing training and awareness programs to build cyber security awareness and capacity.
    - Building incident response capability, including planning and testing of cyber security responses.
- All staff of NSW public service agencies –
    - Understanding the cyber security responsibilities of their role.
    - Following the relevant cyber security policies and procedures in their organisation.
    - Ensuring that cyber security is integrated into work processes, systems and services.
    - Reporting security weaknesses or incidents to the organisation's CISO.

3 Preparedness

3.1 The 2017 State Level Emergency Risk Assessment identifies business continuity planning as a top priority to mitigate the impact of a range of hazards. Cyber incidents are an increasingly important part of organisational risk management and incidents will require careful business continuity planning.

3.2 NSW Government agencies and state-owned corporations are responsible for developing and maintaining cyber incident response plans and business continuity plans that address the risk of a cyber incident to ensure delivery of government services. Agencies should also encourage business, non-government organisations and local government in their areas of responsibility to develop and maintain business continuity plans including cyber incident response plans.

Governance

3.3 Administrative structures for national and state levels of government to manage all aspects of cyber incidents are relatively new and still evolving.

National

3.4 By nature, significant cyber incidents may cross jurisdictional boundaries. Accordingly, NSW actively contributes to a national, cooperative approach to cyber crisis planning.

3.5 National whole-of-government arrangements are described in the Commonwealth Government's *Cyber Incident Management Arrangements* (CIMA).

3.6 Section 5 explains how NSW intersects with national governance arrangements.

New South Wales

3.7 All NSW Government agencies are responsible for ensuring they are adequately prepared for responding to and recovering from cyber incidents. This includes:

- having strong cyber incident response plans and business continuity and surge plans in place (and regularly tested)
- consideration of flexible workplace and workforce arrangements
- a shared understanding amongst senior leaders of governance arrangements and how agency services will be prioritised.

3.8 The GCISO has also established new governance arrangements comprising agency executive leadership to ensure coordinated and risk-based decision-making. The GCISO also supports the Minister for Finance, Services and Property through regular updates for the Counter Terrorism, Emergency Management and Community Safety (CTEMCS) Cabinet Sub-Committee.

3.9 **Cyber Security Senior Officers' Group (CSSOG)**

GCISO has established this Group comprised of senior leadership from all clusters, chaired by Department of Premier and Cabinet with DFSI as Deputy Chair. CSSOG is designed to shift ownership of cyber risk management from IT departments to executive leadership of agencies. CSSOG provides strategic oversight for cyber risk management in NSW Government. It seeks to

understand cyber risks including vulnerabilities, threats and impacts, and leads and coordinates strategies, policies and other arrangements to address these risks.

CSSOG reviews cyber risk management arrangements to ensure there is a comprehensive and integrated WoG strategy for NSW. It supports the Counter Terrorism, Emergency Management and Community Safety (CTEMCS) Cabinet Sub-Committee in its responsibilities for oversight and development of the State's preparedness for acts of terrorism.

3.10 ICT & Digital Leadership Group (IDLG)

The ICT & Digital Leadership Group (IDLG) is comprised of all cluster CIOs and the Government Chief Information and Digital Officer (GCIDO). It considers strategic issues relating to WoG ICT and Digital Government.

The IDLG is responsible for making decisions about mitigating technology risks including cyber risks.

3.11 Cyber Security Steering Committee (CSSG)

The Cyber Security Steering Committee (CSSG) consists of Cluster Chief Information Security Officers (CISOs) or equivalent, a representative from the General Counsel and the Government Chief Information Security Officer (GCISO). It considers issues relating to Cyber risk and security management; driving cultural change across government; ensuring effective risk controls; ensuring appropriate roles and responsibilities are discharged across government; WoG capability uplift.

The CSSG is responsible for making recommendations to the CSSOG and IDLG about mitigating cyber risk.

3.12 Cyber Security Advisory Council (CSAC)

GCISO has established a permanent independent advisory group on cyber security. The purpose of the CSAC is 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 risk, technology, people and process dimensions of cyber security.

CSAC provides expert advice about trends and opportunities in cyber security; recommends options and approaches to emerging cyber trends and issues; and provides opinions and recommendations on specific issues put to it by the GCISO.

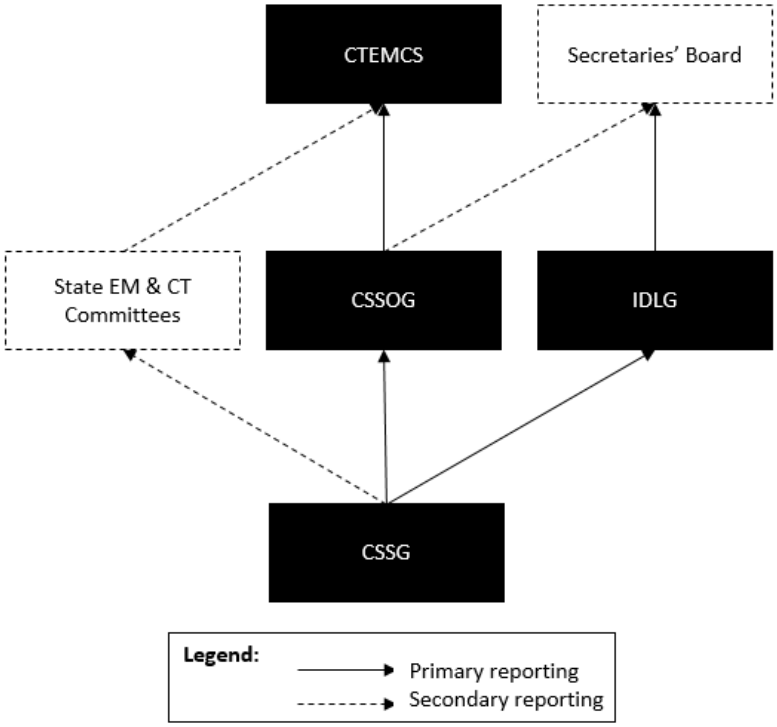

Figure 2: Cyber Security Governance (non-operational)

NSW Capability

3.13 NSW maintains capabilities to prevent, prepare for, respond to and recover from emergencies. The development and maintenance of NSW capability is shared across government agencies consistent with their core responsibilities.

3.14 A cyber emergency poses additional challenges to the 'traditional' emergency due to its unpredictable nature, likely rapid onset and propagation, wide-ranging impacts and prolonged duration (likely many months).

3.15 **During a cyber emergency, all NSW Government agencies are responsible for maintaining core business to the greatest extent possible, according to agencies' cyber incident and business continuity plans, as well as undertaking emergency-related roles identified in the *NSW State Emergency Management Plan* and sub/supporting plans.**

3.16 NSW Government capabilities specific to a cyber emergency response are detailed in Section 5.

Exercise management

3.17 Agencies are strongly encouraged to participate in exercises designed to test their incident management and business continuity arrangements.

3.18 The *NSW Cyber Incident Response Plan* will be regularly exercised. Like physical emergencies or terrorism, a significant cyber security incident or a cyber security crisis can impact community safety, critical infrastructure services and the economic prosperity of NSW. Accordingly, regular briefings are conducted to 'walk through' examples of significant cyber security incidents and

cyber security crises. These exercises allow decision-makers to practice, consider and discuss the interaction between Emergency Management, NSW Police Force and the *NSW Cyber Incident Response Plan*, together with Commonwealth roles and responsibilities, communication protocols when services and systems are impacted, and recovery.

3.19 Plans will be revised as necessary following exercise debriefing sessions (and should be revised following a *Post Incident Review* for genuine incidents).

Financial arrangements

3.20 Expenditure of funds by agencies during cyber emergency response or recovery operations will be met in the first instance by existing operating budgets or arrangements with NSW Treasury. Should the expenditure be of such a magnitude as to prevent the providing agencies from continuing their normal operations for the remainder of the financial year, Treasury may provide supplementation, however agencies cannot be guaranteed that funding will be provided.

4 Detection, threat sharing and reporting

4.1 Unlike physical emergencies, many cyber threats can be rapidly detected and neutralised through vigilant threat sharing and detection.

4.2 The GCISO is provides advice to support agency response teams and sharing information on threats to enable agencies to rapidly take protection measures. This has been implemented via cyber security email alerts and a mobile app. It is strongly recommended that agencies implement the actionable intelligence provided by the GCISO for prevention or detection.

4.3 The *NSW Information Security Event Reporting Protocol* has been defined and is being strengthened. It requires NSW Government agencies to report on events, incidents, near misses and vulnerabilities, and to share information security experience and knowledge. It is aimed at minimising the impact of incidents and enhancing the Government's emergency response and business continuity planning.

Notification

4.4 The *NSW Cyber Incident Response Plan* outlines the notification process within the cyber security community for incidents.

4.5 The GCISO will coordinate all notifications to the cyber security community as per the *NSW Cyber Incident Response Plan*.

Significant Cyber Incident

4.6 The arrangements under the *NSW Cyber Incident Response Plan* for coordination and communication during a significant cyber incident are shown in Figure 3.

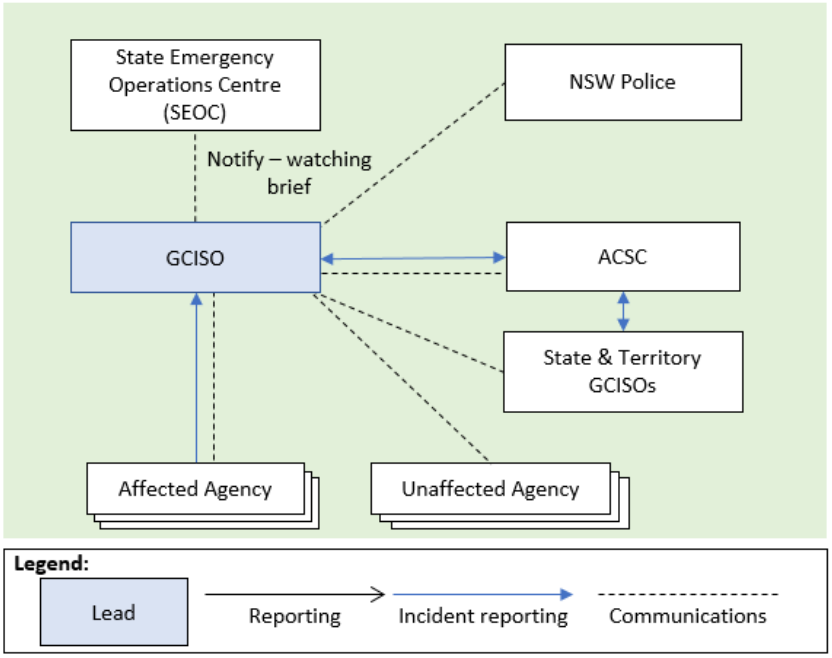

Figure 3: Significant Cyber Incident responsibilities and communication

4.7 The GCISO will notify the State Emergency Operations Centre (SEOC) of any cyber security incident that poses a *potential* threat to people, property or the environment in NSW.

4.8 The SEOC will provide information to the SEOCON and the emergency management sector on any current actions and forecast impacts as advised by the GCISO.

4.9 The ECSOC will coordinate notification to the cyber security community as per the *NSW Cyber Incident Response Plan*.

Cyber Crisis

4.10 The GCISO will notify the State Emergency Operations Centre (SEOC) of any cyber security incident that is a *real and credible* threat to people, property or the environment in NSW.

4.11 The SEOC will provide information to the SEOCON and the emergency management sector on any current actions and forecast impacts as advised by the GCISO.

4.12 If the SEOCON and the GCISO determine that the incident constitutes an emergency, the SEOC will notify the State Emergency Management Committee (SEMC) and seek liaison officers as required by the SEOCON.

4.13 The SEOC will notify Regional Emergency Operations Controllers of activities occurring at state level and assumption of state level control by the SEOCON.

5 Response

5.1 The NSW Government and its agencies are responsible for the whole-of-government operational response to a significant cyber incident or crisis affecting NSW Government systems or services. The NSW Government will work with the Australian Government and other jurisdictions to coordinate information sharing, decision making, and communication strategies as described in the Commonwealth *Cyber Incident Management Arrangements* (CIMA).

Control and Coordination

5.2 Cyber crisis incident management arrangements for NSW are indicated in Figure 4. Details for each entity are provided below.

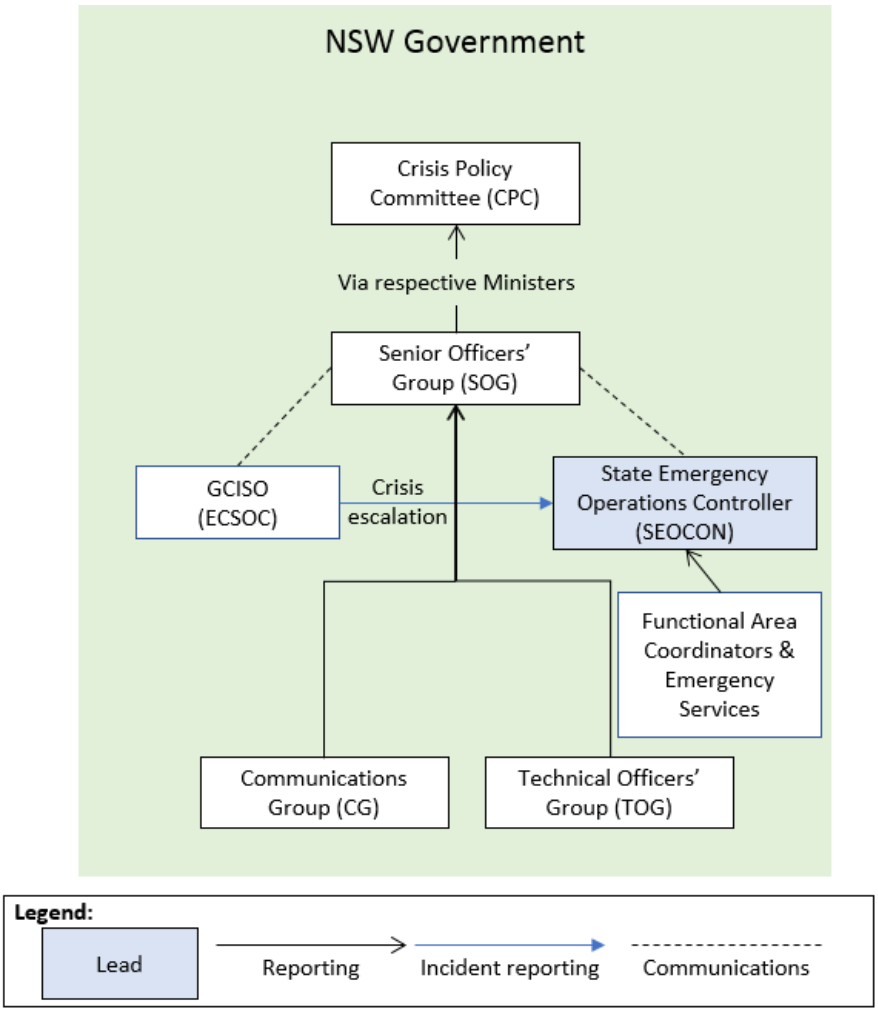

Figure 4: Cyber Crisis response process – NSW

5.3 National coordination arrangements are shown in Figure 5. Further details are provided below.

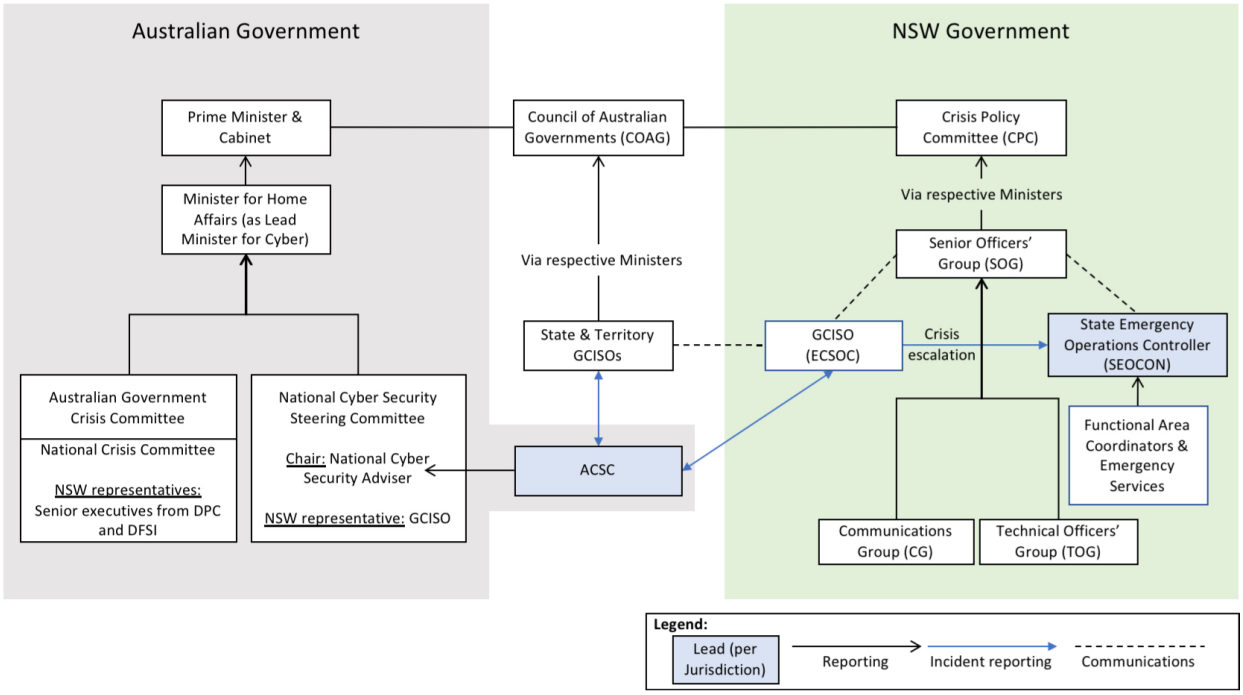

Figure 5: Cyber Crisis response process – National

Responsibilities

NSW Department of Finance, Services and Innovation

5.4 In the event of a cyber security crisis the NSW Department of Finance, Services and Innovation (DFSI) will:

(i) Lead the NSW response to the impacts on NSW Government digital assets.

(ii) Represent NSW on the National Crisis Committee (with NSW Department of Premier and Cabinet).

Emergency Cyber Security Operations Coordinator (ECSOC)

5.5 In the event of a significant cyber security incident or cyber security crisis the Government Chief Information Security Officer (GCISO) within DFSI will assume the role of Emergency Cyber Security Operations Coordinator (ECSOC).

5.6 The ECSOC will:

(i) Provide actionable threat intelligence and advice for threat detection, control or neutralisation across NSW Government.

(ii) Coordinate, develop and maintain a whole of government assessment of the scale and nature of the cyber incident in terms of its cause, spread, cyber impacts.

(iii) Receive feedback and report on mitigation measures across Government to safeguard NSW Government digital information, assets and services and minimise harm to the

community.

(iv) Represent NSW on the National Cyber Security Steering Committee.

(v) Be the principal point of contact with the Commonwealth in terms of sharing information about the cyber incident and any proposed Commonwealth actions.

(vi) Liaise with affected NSW Government agencies on actions being taken to resolve any cyber incident and determine an overall response to the cyber aspects of the incident.

(vii) Identify capability and capacity issues relevant to the NSW cyber incident response.

(viii) Liaise with agency business continuity managers to ensure that they understand how the cyber incident may affect agency operations.

(ix) Ensure the SEOCON and PIFAC are kept advised of the current and anticipated consequences of the cyber incident to support their functions under the EMPLAN.

(x) Advise the NSW Government as required as to the above and make relevant recommendations for whole of government action to safeguard information, assets and services and minimise the impact of the event.

(xi) Advise the NSW Government as to the need to convene the Crisis Policy Committee.

(xii) Deploy a Liaison Officer to the State Emergency Operations Centre if operational.

NSW Department of Premier and Cabinet (DPC)

5.7 The NSW Department of Premier and Cabinet will represent NSW on the National Crisis Committee (with DFSI).

State Emergency Operations Controller (SECON)

5.8 In the absence of a prescribed combat agency for a significant cyber security incident or cyber security crisis, the SEOCON will when requested by the ECSOC take responsibility for the control and coordination of consequence management for the incident as per the EMPLAN.

Crisis Policy Committee (CPC)

5.9 Following identification of an emerging cyber crisis, the SEOCON can request that the Premier convene the Crisis Policy Committee (CPC).

5.10 The CPC will provide overarching strategic policy leadership and make decisions to address the implications and manage the risks of a cyber crisis and determine the whole-of-government public communications strategy.

- This could include, for example, determining whether to take extreme actions to limit the spread of malware or to prioritise staff to support critical services while shutting down non-critical services.
- Chaired by the Premier, the Crisis Policy Committee's membership includes Ministerial representatives of key relevant portfolios, plus relevant Commissioners and Secretaries as required and invited by their Ministers. The proposed membership for a cyber crisis response is included at Appendix 1.

5.11 The severity of the cyber crisis will determine the CPC's level of activity. The group may meet on

an ad hoc basis, as required by major shifts in the incident response (e.g., while impacts to the community are under control), or more regularly (e.g., weekly or daily) if needed.

5.12 The decisions of the CPC may be informed by options and recommendations prepared by the SECON, ECSOG or SOG.

Australian Cyber Security Centre (ACSC) and Joint Cyber Security Centre (JCSC) – Sydney

5.13 Coordination arrangements are in place between the GCISO and the Commonwealth Joint Cyber Security Centre (JCSC) Sydney node. The JCSC is a part of the Australian Cyber Security Centre (ACSC). These arrangements enable the ECSOC to convey cyber incident information to and receive cyber incident information from the Commonwealth and private sector (particularly banking and telecommunications firms) to ensure SEOCON has a comprehensive and consistent understanding of an incident as it unfolds.

Senior Officers Group (SOG)

5.14 During an emergency resulting from a cyber security incident the Senior Officers Group (SOG) – a subset of the CSSOG – is formed. Under a cyber crisis the SOG is chaired by the ECSOC.

5.15 The SOG is responsible for activating their business continuity plans to take required response actions, briefing their respective cluster Secretaries/Ministers on the actions and broader communications provided by the ECSOC.

5.16 SOG members must ensure their agencies' cyber incident and business continuity responses are appropriately resourced by identified teams within each agency.

5.17 If the NSW Crisis Policy Committee (CPC) has convened in relation to the incident, the SOG will provide strategic-level briefings to the Crisis Policy Committee via the ECSOC to inform Ministerial decision-making. The SOG will escalate complex and significant policy matters to the CPC and provide advice on these matters.

5.18 The Premier may convene a joint session of the CPC and SOG as needed.

Technical Officers Group (TOG)

5.19 During an emergency resulting from a cyber security incident, a Technical Officers Group (TOG) – a subset of the IDLG and the CSSG – is responsible for forming a WoG view of the scale and nature of the cyber incident in terms of its spread, impacts (including on the NSW community) and likely duration. It is chaired by the Director of Cyber Security Operations (who reports to the ECSOC).

5.20 CIO members of the TOG are responsible enabling their respective CISOs or other relevant staff take required response actions, briefing their respective members of the SOG on their actions.

5.21 During a cyber security crisis, extraordinary action may be required to be taken to protect ICT assets and networks from an imminent or ongoing threat. CIOs will take all reasonable actions to ensure this occurs if requested by the ECSOC, the Crisis Policy Committee (CPC), or when a direction is made under the *State Emergency and Rescue Management Act 1989* or other relevant act of Parliament.

Public information and the Communications Group (CG)

5.22 During a cyber crisis, the Communications Group (CG) is activated. It is chaired by the Public Information Functional Area Coordinator (PIFAC) and members include Cluster

media/communications representatives who should be familiar with the Public Information Functional Area arrangements established under the NSW Emergency Management Plan, and the Director Cyber Security Engagement and Prevention.

5.23 Via the CG, the PIFAC will coordinate public information and all media interaction, reporting messaging and media events to the SOG.

5.24 The Director Cyber Security Engagement and Prevention (the ECSOC's delegate) will liaise with affected NSW Government organisations to advise the PIFAC in relation to messaging for the incident. They will coordinate regularly and work closely with the PIFAC to ensure consistency of information across NSW Government organisations.

5.25 During and following a significant cyber security incident or cyber security crisis, the release of information to the public will need to balance the competing interests of transparency with the sensitivities necessary for response and operational requirements.

NSW Government organisations

5.26 Unless otherwise outlined in the EMPLAN and any other Supporting Plans, NSW Government organisations remain responsible for their own IT systems, services, infrastructure, business continuity, cyber security response and disaster recovery.

5.27 Agency responsibilities for reporting incidents to the GCISO are outlined in the *NSW Cyber Incident Response Plan.* Coordination and communication during a significant cyber incident were shown in Figure 3. Most importantly all NSW agencies are required at all times to:

- Report incidents to the GCISO in a timely manner – as defined in the *NSW Cyber Incident Response Plan.*
- Undertake threat detection and monitoring in response to alerts provided by the GCISO.
- Share threat intelligence with the GCISO to enable WoG communication.

5.28 In the event of a significant cyber incident or an emergency caused by a cyber crisis all NSW agencies will also:

- Implement threat mitigation and/or incident response plans.
- Collaborate across Government to support other affected agencies as needed.

5.29 In the event of a significant cyber incident or an emergency caused by a cyber crisis, *affected* NSW Government organisations will also be required to:

- Develop and maintain an assessment of the scale and nature of the cyber incident in terms of its spread and impacts, and report this to the ECSOC.
- Report current and planned activities to the ECSOC.
- Implement any reasonable requests made by the ECSOC as part of a multi-agency or emergency response.

5.30 During a significant cyber security incident or crisis, individual NSW Government agencies affected are responsible for response within their agencies. This should be done in a coordinated manner. Cluster CISOs and/or SROs where applicable will be expected to respond under the coordination of the ECSOC or their delegate regarding cyber security incident response planning.

NSW Police Force

5.31 If a cyber security incident has the potential or is determined to be an actual criminal act, the NSW Police will assume a greater level of control over the cyber incident response operations.

5.32 NSW Police will provide advice to the SEOCON and TOG on preservation of evidence in relation to any emergency management operations occurring.

Emergency Services Organisations

5.33 The roles and responsibilities of Emergency Services Organisations during a major emergency, such as a significant cyber security incident or a cyber security crisis affecting NSW Government organisations, are those as outlined in the EMPLAN and any other Supporting Plans.

Functional Areas

5.34 The roles and responsibilities of Functional Areas during a major emergency, such as a significant cyber security incident or a cyber security crisis affecting NSW Government organisations, are those as outlined in the EMPLAN and any other Supporting Plans.

The Treasury (NSW Industrial Relations)

5.35 NSW Industrial Relations will provide advice to the Secretary of Treasury, in the role of Industrial Relations Secretary, and to government sector agencies on working arrangements in place in the event of a cyber emergency, in accordance with the NSW Government's Memorandum of Understanding with Unions NSW.

Stand Down

5.36 The ECSOC will notify the SEOCON if it is determined that a significant cyber security incident or a cyber security crisis affecting NSW Government organisations no longer exists. The SEOCON may require continued support from the GCISO if the consequences of the incident are ongoing.

6 Recovery

6.1 The NSW Recovery Plan outlines the strategic intent, responsibilities, authorities and the mechanisms for disaster recovery in NSW.

6.2 Responsibility for coordination of recovery operations in NSW rests with State Emergency Recovery Coordinator (SERCON), or as otherwise specified in specific emergency plans.

6.3 Following an emergency resulting from a significant cyber security incident, a recovery committee may be formed for strategic coordination of recovery activities. The GCISO/ECSOC will be invited to participate on the recovery committee.

GCISO/ECSOC

6.4 As part of a coordinated recovery process the GCISO/ECSOC will be responsible for ongoing coordination between the SEOCON and the cyber security community. They will:

(i) seek estimated recovery timeframes for network and key government information systems

(ii) facilitate coordination of recovery information between the government and the private sector

(iii) support any ongoing Public Information strategy throughout the recovery process.

Government organisations

6.5 Following a significant cyber security incident or crisis, individual NSW Government agencies affected are responsible for recovery operations within their agencies. This should be done in a coordinated manner.

6.6 A cyber security specific recovery sub-committee may be established by the recovery committee.

6.7 NSW Government organisations, specifically CSSOG members, maintain responsibility for their own business continuity and disaster recovery and notify the GCISO/ECSOC of these actions and resulting service level improvements.

6.8 The Cyber Security Advisory Council (CSAC) will provide the GCISO with expert advice from outside of NSW Government regarding the impacts of specific significant cyber security incidents or crises and suggested recovery strategies.

Post incident Reviews

6.9 GCISO will coordinate a WoG post cyber incident review, including recommendations. CISOs and the Cyber Security Steering Group (CSSG) will provide relevant information to assist in the compilation of this review. The ICT and Digital Leadership Group (IDLG) comprising CIOs will consider and endorse recommendations of the review. The Cyber Security Senior Officers' Group (CSSOG) will drive the recommendations across clusters to reduce impacts from the specific significant cyber security incident or crisis, and to inform preparation and prevention for future incidents.

6.10 The GCISO will participate in the emergency management operations After Action Review process.

Appendix 1: Crisis Policy Committee membership

The following is the proposed membership of the CPC:

- Premier (Chair)
- Deputy Premier
- Treasurer
- Attorney-General
- Minister for Emergency Services – Minister for Police
- Minister for Finance, Services and Property
- Minister for Counter Terrorism
- Minister for Health
- Secretary, Department of Premier and Cabinet Secretary
- Secretary, Department of Finance, Services and Innovation
- Secretary, Department of Health
- Secretaries and Ministers of Departments most affected by the incident and experiencing the highest impact on the NSW community
- NSW representatives on the National Crisis Committee (senior officials from Department of Premier and Cabinet and DFSI)

Other Ministers and senior government officials may be invited at the request of the Premier.

Appendix 2: Glossary

Combat Agency	A combat agency is an individual NSW agency identified as responsible for controlling emergency response operations for a specific hazard. Combat Agency has the same meaning as in the EMPLAN.
Crisis Policy Committee	The NSW Government strategic level committee convened by the Premier in the event of a crisis in NSW. The Crisis Policy Committee consists of the Premier, key Ministers, Cluster Secretaries and other essential advisors as required by the incident.
DDOS	Distributed Denial of Service. A DDOS attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
Emergency Operations Centre	Emergency response supporting operations are coordinated through an Emergency Operations Centre. Emergency Operations Centre has the same meaning as in the EMPLAN.
Emergency Services Organisations	Emergency Services Organisations perform a range of emergency management functions in NSW and include organisations such as the NSW Police Force, Fire & Rescue NSW, the NSW Rural Fire Service, Ambulance Service of NSW and NSW State Emergency Service. Emergency Services Organisations has the same meaning as in the EMPLAN.
EMPLAN (NSW State Emergency Management Plan)	The EMPLAN gives a strategic overview for emergency management in NSW. This Sub Plan is prepared to support the EMPLAN.
Functional Area	Functional Areas represent key NSW sectors which provide support in emergency response. Functional Area has the same meaning as in the EMPLAN.
SEOC (State Emergency Operations Centre)	An Emergency Operations Centre established by the SEOCON.
SEOCON (State Emergency Operations Controller)	The SEOCON is a member of the NSW Police Force Senior Executive Service and is responsible for the control and coordination of emergency response operations at the state level for which the SEOCON is the designated controller or where there is no dedicated Combat Agency (among other responsibilities). Has the same meaning as in the EMPLAN.
SERCON (State Emergency Recovery Controller)	The SERCON is the Chief Executive Officer of the Ministry for Police and Emergency Services and is responsible for a range of emergency recovery arrangements as outlined in the EMPLAN.
Supporting Organisations	The Government Departments, statutory authorities, volunteer organisations and other specialist agencies who have indicated a willingness to participate and provide specialist support resources to a combat agency Controller or Functional Area Coordinator during emergency operations.