GOVERNMENT OF WESTERN AUSTRALIA

SEMC
STATE EMERGENCY MANAGEMENT COMMITTEE

Cybersecurity Incident

STATE HAZARD PLAN

Interim

RESPONSIBLE AGENCY
Department of the Premier and Cabinet

APPROVED BY
State Emergency Management Committee

RESOLUTION NUMBER	17\2021
VERSION NUMBER	INTERIM V 1.01
DATE OF APPROVAL	27 FEBRUARY 2026
DATE OF EFFECT	01 MARCH 2026
REVIEW DATE	MARCH 2027

Acknowledgement of Country

The State Emergency Management Committee (SEMC) acknowledges the Aboriginal peoples throughout the state of Western Australia as the Traditional Custodians of the lands where we live, work and volunteer. We recognise Aboriginal peoples' continued connection to land, waters and community, and pay our respects to Elders both past and present.

Contact Details

Principal address:
Dumas House
2 Havelock Street
West Perth WA 6005

Postal address:
Locked Bag 3001
West Perth WA 6872

Contacts
Telephone: (08) 6552 5000
Fax: (08) 6552 5001
Email: Cyber.Policy@dpc.wa.gov.au

Amendments Table

Date	Details	Amended by
December 2024	Interim Version 1.00 - SEMC approved 4 December 2024 (resolution 101/2024).	Department of the Premier and Cabinet
March 2026	Interim Version 1.01 - SEMC executive officer approved statement of fact amendments (resolution 17/2021) to align with the formal prescription of cybersecurity incident as a hazard within the EM Regulations and updates to WA and national cybersecurity frameworks and strategies.	SEMC Business Unit

This document was designed to be viewed electronically and aims to meet the West Australian Government's accessibility and inclusivity standard, including meeting the World Wide Web Consortium's Web Content Accessibility Guidelines version 2.1 (WCAG 2.1) at level AA. If anything in this document is inaccessible to you, or you are experiencing problems accessing content for any reason, please contact the State Emergency Management Committee Business Unit at semc.policylegislation@dfes.wa.gov.au.

All of the State emergency management legislation and documents can be accessed via the State Emergency Management Framework page of the State Emergency Management Committee website.

Contents

Tables

Figures

Part One:

Introduction

This State Hazard Plan – Cybersecurity Incident (The Plan) provides an overview of arrangements for the management of Cybersecurity Emergencies in Western Australia (WA) and contains information on prevention, preparedness, response and initial recovery.

The SHP – Cybersecurity Incident refers to a range of existing plans and documents relating to cybersecurity. It does not duplicate the information contained in these, instead providing directions to websites or other sources where further information can be obtained if required.

The Department of the Premier and Cabinet (DPC) is the Hazard Management Agency (HMA) for cybersecurity incident.

1.1 Background

Digital technology has transformed almost all aspects of our lives, and the pace of digitisation has rapidly accelerated in recent years. The internet offers significant economic, social and personal benefits and has become crucial to managing our finances, getting an education, conducting business and staying connected. These opportunities are, however, also accompanied by security risks that need to be managed.

While the cyber realm is a critical enabler of improvement in our lives, it also acts as a vector through which malicious actors can cause harm. Cybersecurity threats are increasing in frequency, scale and sophistication, and as a government we must ensure we are capable of preventing and mitigating cybersecurity incidents, as well as responding to and recovering from cybersecurity incident emergencies.

1.2 Scope

The SHP – Cybersecurity Incident covers emergency management arrangements within the geographic boundaries of WA, for the hazard of cybersecurity incidents. It is designed to inform WA stakeholders of prevention and mitigation strategies, preparedness for, response to, and recovery arrangements following the impact of a cybersecurity incident emergency triggered under section 3 of the *Emergency Management Act 2005* (EM Act).

While unlikely to be required for a cybersecurity incident, the EM Act can be used to access emergency powers through the declaration of an 'emergency situation' or a 'state of emergency'. See section 4.6.1 of this plan for more information.

In the absence of an 'emergency situation' or 'state of emergency' declaration, the HMA will offer expert advice, collaborate with and support private industry organisations to manage cybersecurity incidents, working in partnership with relevant portfolio government departments.

WA owners and operators of critical infrastructure within Western Australia captured by the *Security of Critical Infrastructure Act 2018* (SOCI Act) have additional obligations for managing their cyber risks in addition to this Plan.

1.3 Hazard definitions

The definition of a **cybersecurity incident emergency** within this Plan refers to the definition of 'emergency' under the EM Act as the occurrence or imminent occurrence of a hazard which is of such a nature or magnitude that it requires a significant and coordinated response.

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]

A **cybersecurity incident** is defined under the State's *Emergency Management Regulations 2006* (the EM Regulations) r. 14B as an event or situation in which:

(a) an electronic system is modified or impaired

(b) a threat is made that causes a person to have a reasonable suspicion that an electronic system is being or will be modified or impaired

(c) a person reasonably suspects that an electronic system is being or will be modified or impaired.

The terms '**impairs or modifies**' requires that the cybersecurity incident is capable of causing or resulting in:

(a) loss of life, prejudice to the safety, or harm to the health, of persons or animals; or

(b) destruction of, or damage to, property or any part of the environment.

Impair, in relation to an electronic system, includes the following:

(a) to gain unauthorised access to the system or electronic information that is used by, within or in relation to the system

(b) to intercept electronic information that is used by, within or in relation to the system

(c) to prevent the system from properly functioning.

For the purposes of this Plan, **electronic system** is not restricted based on ownership and may include:

- all WA Government entities included in the scope of WA Cyber Security Policy and WA Cyber Security Incident Framework (Public service, WA Government Trading Enterprises, WA Universities, Schedule 2 entities[2])
- all critical infrastructure entities
- all entities with mixed private and public ownership
- all private entities
- individuals.

1.4 Organisational roles and responsibilities

The Department of Premier and Cabinet (DPC) is the HMA for the hazard of cybersecurity incident. The following positions within DPC have been authorised to act in the name of the HMA in the roles and functions as prescribed in sections 50, 53, and 55(1) of the EM Act:

- Director General of the Department of the Premier and Cabinet
- Government Chief Information Officer.

DPC is also the Controlling Agency for the hazard of cybersecurity incident. The Office of Digital Government (DGov), within DPC is responsible for carrying out the functions of the Controlling Agency on behalf of DPC.

Information regarding the roles and responsibilities of relevant agencies under the Plan are detailed in Appendix C.

It is recommended that each entity with a role or responsibility under this Plan has appropriate operational procedures detailing their response arrangements in accordance with the Plan.

These arrangements should be complementary to the entity's operational procedures detailing their roles and responsibilities under the State Emergency Management Plan (State EM Plan).

Notes

1 NIST Privacy Framework Version 1.00
2 A schedule 2 entity is defined in the *Public Sector Management Act 1994* (WA).

1.5 Related documents and legislation

This Plan is to be read in conjunction with the State Emergency Management Framework, including the EM Act, the EM Regulations, State Emergency Management Policy (State EM Policy), plans and procedures.

In addition, the Plan is to be read in conjunction with the following documents:

- Western Australian Government Cyber Security Policy and guidance
- Western Australian Government Cyber Security Incident Coordination Framework (CSICF)
- Australian Government Cyber Incident Management Arrangements
- Australian Government Protective Security Policy Framework (PSPF)
- Australian Cyber Security Centre cyber security guidance

Legislation and guidance relevant to this Plan include but are not limited to:

- *National Emergency Declaration Act 2020* (Commonwealth)
- *Security of Critical Infrastructure Act 2018* (Commonwealth) – Part 3A 'Responding to serious cyber security incidents'
- *Privacy Act 1988* (Commonwealth)
- *Privacy and Responsible Information Sharing Act 2024*
- *Data Availability and Transparency Act 2022* (Commonwealth)
- *Cyber Security Act 2024* (Commonwealth) (Limited Use Obligations).

1.6 Security assurance

Security assurance activities are designed to validate that practices, procedures, and architecture are in place and are continuously improved to support HMA's compliance with legal obligations under the EM Act.

DPC, through DGov, undertakes the following assurance initiatives detailed in **Table 1.**

Area	Activities	Tools
WA Government Cyber Security Policy	Prescribes the establishment and maintenance of essential cyber security capabilities for WA government covering hazard prevention, mitigation and incident response	**Prevention** · Cyber Security governance, management and security operations standards · Prescribed cyber security controls · Essential cyber security operational capability for WA government entities · Requirement to consider information security risks of procurement, and have cyber security contract clauses in procurement contracts · Essential standards for data offshoring, cloud security management, enterprise mobility, secure data removal and device disposal, vulnerability management program, encryption, physical security of assets and personnel security · Requirement to manage Artificial Intelligence security and establish a roadmap to Post-Quantum cryptographic standards · Requirement to consider security of Internet-of-Things devices and Operational Technology · Requirement to report any cybersecurity incident to Office of Digital Government (applies regardless of the incident severity level). **Preparedness** · Requirement for staff to undergo cyber security awareness and training · Requirement for entities to participate in regular cybersecurity incident exercises · Requirement for entities to have the capacity to undertake continuous incident monitoring and adverse event analysis to detect and diagnose cybersecurity incidents. A requirement to be connected to Western Australian Security Operations Centre managed by DGov · Requirement to have the ability to undertake analysis of the entity's cyber security context and risk management · Essential standards for detecting and diagnosing a cybersecurity incident · Requirement to establish entity cybersecurity incident management and response plans · Requirement to establish the entity's capability to recover from the impact of a cybersecurity incident.

Area	Activities	Tools
Cyber Security Incident Coordination Framework	Develops a structured coordination process for management of cybersecurity incidents in WA Government	**Incident Response** · Definition of cybersecurity incident thresholds · A structured coordinated approach to management of cybersecurity incidents from cybersecurity incident identification to response and recovery · Details of requirements for escalation of incident responses and reporting.
Training and development of personnel	Ongoing training and awareness Horizon scanning and continuous improvement in the contemporary understanding of the hazard	**Prevention and Preparedness** · Cyber security and awareness training · Cyber capability development support · Regular updates on threat changes in the cyber security landscape · Whole-of-government cyber security advisories · Threat hunting and diagnosis · Engagement at interjurisdictional and national levels · Monthly trends and issues: mitigation, response and recovery training · Dark Net monitoring · Cyber security exercises including development of mandated Cyber Security emergency management exercises under State Hazard Plan – Cybersecurity Incident. **Incident Response** · Incident response best practice advisory · Independent breach response playbook review · Breach response – tabletop exercises.
Testing systems and processes	A consistent and structured approach is applied to all aspects of operational performance	**Prevention and Preparedness** · Specialist profiling and alerting · Penetration testing · Vulnerability scanning · Security Operations Centre (SOC) testing and validation tools.

Area	Activities	Tools
Procurement	Information security built into procurement processes	· The Office of Digital Government Information Secure Procurement Framework · Information Secure Procurement & Supply Chain Risk Management guidance and risk assessment templates · Supplier assurance advisory services.
Annual Implementation Report	As a requirement of the WA Government Cyber Security Policy, government entities are required to report yearly against their implementation of the Policy and Essential Security Controls to DGov. This provides a sector wide view on the maturity of agencies and assists to direct resources to building capability in the areas which are most needed.	· WA Government Cyber Security Policy Annual Agency Implementation Reports · Review and analysis of entity OAG management letters, which supports design and prioritisation of targeted capability uplift programs, identifies opportunities for whole-of-government solutions and informs direct engagement with entities to remediate significant findings.
Continuous improvement	Operational performance is reviewed to ensure ongoing effectiveness	· Targeted Cyber Security Capability Uplift engagements · Collecting and analysing performance and assurance data (such as Annual Implementation Reports (AIR) and analysis of OAG Management Letters) · Delivery of training and awareness programs · Facilitation of exercises and incident preparedness activities · Regular review of cyber security arrangements to support incremental enhancements to the sector's cyber security capabilities · Capability uplift, legacy assets and service continuity management advisory.

Table 1. Cyber security assurance activities

Part Two:

Prevention and Mitigation

Prevention, mitigation and preparedness activities for the cybersecurity incident hazard occur at multiple levels.

2.1 State prevention and mitigation strategies

DPC is the HMA for the hazard of cybersecurity incident and is responsible for undertaking prevention and/or mitigation activities within WA and coordination with national bodies to ensure that the strategies are consistent with national priorities and standards.

This includes development of advice, direction, coordination, and support of whole-of-government cyber security efforts to protect the WA government's information, assets, and service delivery from cyber threats.

This function is administered through DGov who undertakes prevention and mitigation strategies, including:

- Engaging with national cyber security coordination bodies, including the Australian Cyber Security Centre (ACSC), to share threat and risk intelligence
- Aligns WA Government controls, guidance and uplift activities with national frameworks
- Incorporates national threat intelligence into WA SOC monitoring, vulnerability scanning and threat-hunting activities
- Coordinates and supports national cyber incident reporting to the ACSC
- Contributes to joint response and investigation activities where required
- Uses national lessons learned and advisories to strengthen state-level guidance, uplift programs, exercises and incident coordination arrangements
- Ensures WA Government entities benefit from nationally identified threats, mitigations and good practice through policy, guidance and capability uplift.

Accountable authorities (CEOs, Directors General or chief employees) are responsible for overall cyber security risk management for their entity. This includes ensuring the implementation and prevention and mitigation activities described in Table 2.

Area	Activity	Detail
Govern/ Establish	Accountability	• Understand entity and accountability for cyber security arrangements, including when they are outsourced • Appoint a security executive that has the executive responsibility for cyber security of the entity. • Establish entity cyber security governance, governance of Annual Implementation Reporting to DGov.
	Cyber security operations	• Establish an area or function performing cyber security operations.
	Prescribed cyber security controls for entities	• Governance of implementing cyber security controls as outlined by WA Cyber Security Policy, in alignment with Maturity Level 2 of ACSC Essential Eight Cyber Security Controls (Australian Cyber Security Centre, ACSC) and Zero Trust Principles) and governance of Annual Implementation Reporting (AIR) against implementation of the Policy to the Office of Digital Government • Governance of processes to address Office of Auditor General cyber security findings.
Identify	Risk assessment	• Identify the entity's assets, platforms, applications, software, procurement partnerships, privileged access and identity management practices and any other systems, engagements and activities that may be associated cyber security risks. • Adopt a holistic risk management approach that considers the sensitivity of the information held, the criticality of the services provided and system vulnerabilities.
	Risk management	• Develop a cyber security plan which identifies priorities, constraints, risk tolerances, assumptions and established risk management processes. • Assess and manage business continuity risks. • Develop entity's internal cyber security documents (policy, guidance, procedures) • Manage risks across all entity systems, including (but not limited to) enterprise mobility, artificial intelligence use, internet-of-things devices, operational technology, software development, as well as physical and personnel security. • Manage Limited Use Obligations ensuring that any communications relating to cyber security incidents which was communicated to the Australian Cyber Security Centre (Commonwealth Government) is labelled Official: Sensitive Legal (Limited Use).

Area	Activity	Detail
Protect	Cyber vulnerability management	· Establish prescribed cyber security controls · Develop and implement cyber security vulnerability management processes · Connect to WA Cyber Security Operations Centre. · Implement prescribed controls to ensure vulnerability management, cyber secure enterprise mobility, procurement, data offshoring, device disposal, encryption, physical security and personnel security practices · Implement entity roadmaps towards the establishment of Post Quantum Cryptographic Standards · Implement Artificial Intelligence security controls · Data Offshoring Security.
	Cyber security awareness and training	· Staff undertake cyber security awareness training on an annual basis with training for executives, finance/payroll staff, and other staff in sensitive positions being prioritised · Staff in charge of cyber security operations receive training that caters appropriately to their role requirements. · Regular cyber security exercising.
	Secure procurement practices	· Integrate cyber security considerations in the procurement of all digital goods including internet-of-things devices and services, including demonstrating performance of due diligence, supply chain risk management, understanding the service ownership model and inclusion of standard contract clauses (DGov Information Secure Procurement Framework and risk assessment templates). · Consideration of cyber security risks when procuring a cloud solution.
	Information security	· Implementation of the WA Information Classification Policy · Consideration of information security in relation to cloud solutions · Secure software development · Secure procurement of internet of things devices and operational technology.

Area	Activity	Detail
Detect	Monitoring, detection and diagnosis	• Develop appropriate activities to note and identify the occurrence of cyber security incidents. • Event logging • Intrusion detection • Establishing and connecting to a Security Incident and Event Management System (SIEM) • Processes to monitor, analyse and triage security events.
Respond	Responding to an incident	• Report incidents to DGov within 6 hours • Develop and maintain entity cyber security incident management and response plans (ensuring they are printed out and hard copy kept in a secure place) • Developing and maintaining incident response playbooks • Developing and maintaining cyber exercise and testing programs for the entity.
Recover	Recover from the impact of a cyber security incident and restore capability, services and information	• Developing and maintaining capability to restore services and information • Developing and maintaining capability to implement lessons learnt processes.

Table 2. Prevention and mitigation strategies for cyber security at the state level

The WA Government Cyber Security Policy prescribes the baseline security requirements for the WA Government. Entities not specified in the Scope are encouraged to comply with the provisions of the Policy.

2.2 National prevention and mitigation strategies

Australia's national approach to cyber prevention and mitigation is framed by the 2023–2030 Australian Cyber Security Strategy, which sets a whole-of-nation roadmap to make Australia more cyber resilient by 2030.

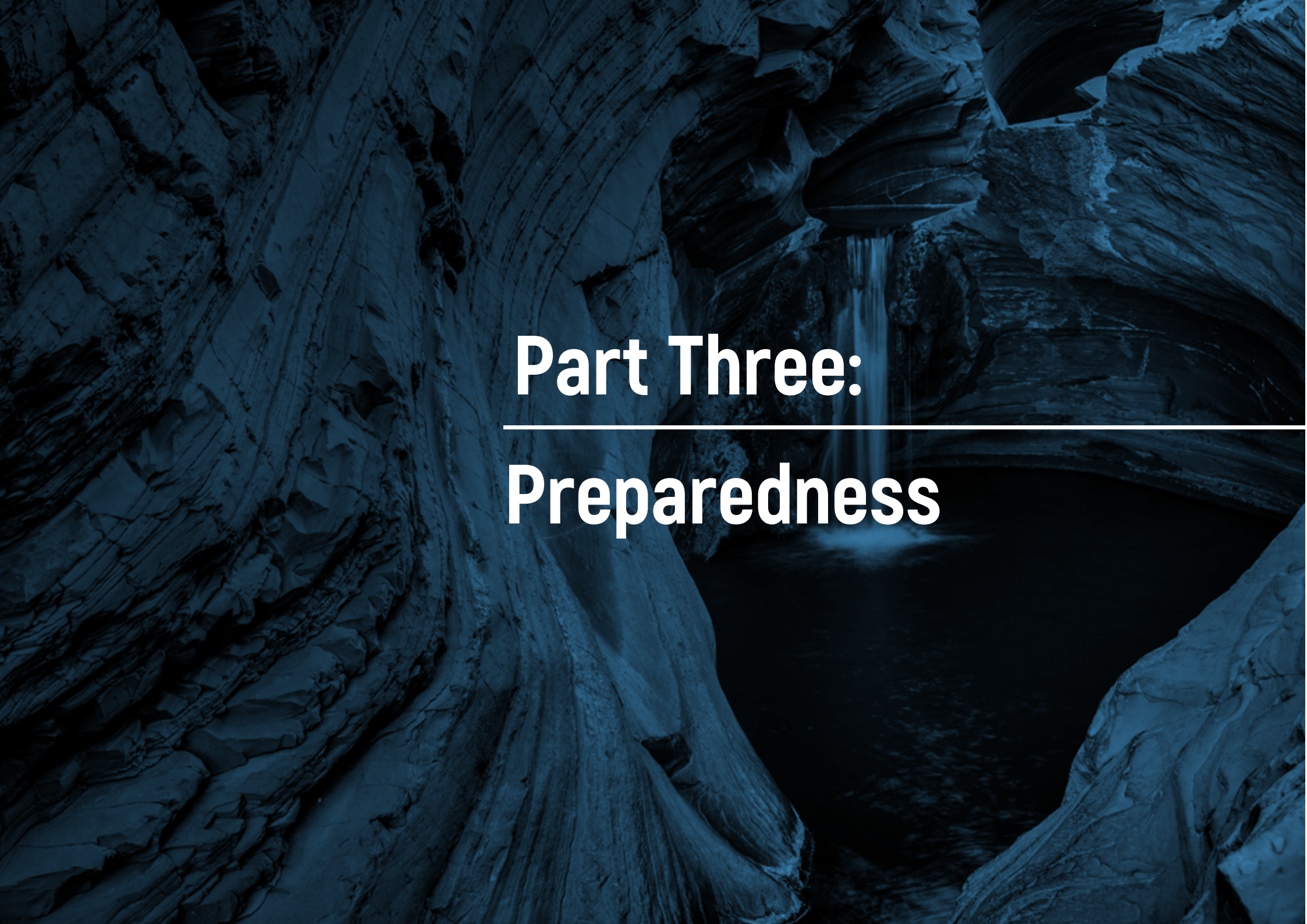
The supporting Action Plan outlines a series of targeted initiatives that operationalise the strategy's goals. This includes:

- Regulatory intervention through the *Security of Critical Infrastructure Act 2018* (SOCI Act) which places risk management and reporting obligations on critical infrastructure owners and operators.
- Baseline Technical Mitigation Controls to promote a nationally consistent approach to the implementation of security controls
- Threat Intelligence Sharing and Disruption including alerts, advisories, and technical guidance to enable early detection and faster mitigation of cyber incidents.
- Incident Response and Impact Mitigation, to support containment, remediation, and recovery from cyber incidents.
- Industry Engagement and Trusted Collaboration provided by the Cyber and Infrastructure Security Centre (CISC) to provide regulatory guidance, sector engagement, and resources to help organisations meet cyber security obligations.
- The Trusted Information Sharing Network (TISN) enables trusted, non-regulatory information sharing across critical infrastructure sectors, supporting collective risk awareness and mitigation of cascading cyber impacts.

2.2.1 Critical Infrastructure including Government Trading Enterprises (GTEs)

The Critical Infrastructure Risk Management Program (CIRMP) is Australia's core regulatory mechanism for engaging critical infrastructure entities on cybersecurity. Established under Part 2A of the SOCI Act, CIRMP requires responsible entities to identify, assess, and manage material risks arising from cyber, physical, personnel, and supply-chain hazards that could have a relevant impact on critical assets. Cybersecurity is explicitly captured as a mandatory hazard area, including risks to operational technology (OT), IT systems, and business-critical data. Entities must maintain a written risk management program, ensure board-level oversight, and submit annual reports to the Department of Home Affairs.

Alongside regulation and operational support, the Australian Government enhances cyber resilience by working with critical infrastructure operators through the Cyber and Infrastructure Security Centre (CISC). CISC offers sector-specific guidance, resources, and communications to help operators manage risks and comply with regulations, translating legal requirements into practical steps and improving coordinated responses across sectors.



Part Three:

Preparedness

3.1 Responsibility for preparedness

As the HMA, DPC is responsible for the development and coordination of preparedness plans and activities for the management of whole-of-government cyber security incidents.

In addition, entities must also have strategies and operational plans in place to prepare for business continuity and consequential emergency responses.

3.2 Capability baseline

The WA Government Cyber Security Policy (the Policy) outlines the baseline capabilities which must be established and maintained. The Policy requires each organisation implement a baseline set of technical controls comprising the Australian Cyber Security Centre's (ACSC's) Essential Eight controls. The Essential Eight controls must be implemented to Maturity Level One as a minimum and agencies are required to report annually on their progress towards this baseline target. An entity may be required to implement higher maturity levels and additional security controls based on their own risk assessment.

3.3 Planning and arrangements

The following plans and arrangements (agreements) have been developed at State and national levels and will be applied as appropriate in the event of a cybersecurity incident emergency.

3.3.1 State arrangements

WA Government Cyber Security Incident Coordination Framework (CSICF)

CSICF is a structured coordinated process for management of cyber security incidents in WA Government, from incident identification to recovery. It contains details of requirements for escalation of incident responses and reporting lines, and details of requirements for escalation of incident responses.

Accountable authorities (CEOs, Directors General or chief employees), assigned under the WA Government Cyber Security Policy, are responsible for managing their entity's risk, which includes cyber risk. They are accountable for developing, maintaining and testing cybersecurity incident response plans and business continuity plans that address the risk of cybersecurity incidents to ensure continuity of 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 cybersecurity incident response plans.

Resources

Resource requirements will depend on the nature, size, complexity and location of the cybersecurity incident emergency. This is consistent with the emergency management principle of a graduated response. The HMA maintains a base level of "business as usual" resources. Outside of this resourcing, and where the HMA has assessed a requirement for more resources, the HMA will draw upon industry and government stakeholders to resource the control structure required for the incident including operational functions, intelligence, capital items and infrastructure.

Organisations with roles and responsibilities identified in Appendix C of this Plan should ensure that they have the necessary and appropriate resources in place to effectively meet their obligations during a Cybersecurity Incident emergency.

3.3.2 National arrangements

The interconnected nature of Information Technology (IT) and Operational Technology (OT) systems and networks increases the likelihood that any major cybersecurity incident will have impacts across multiple jurisdictions. When a Cyber Security Incident emergency occurs and has national implications, the HMA will remain responsible for operational management of the response within WA.

National coordination of cybersecurity incidents will be managed in accordance with the arrangements set out in the Cyber Incident

Management Arrangements for Australian Governments (CIMA) and the supporting CIMA operating Handbook shown in Figure 1. The CIMA works within the context of the Australian Government Crisis Management Framework to ensure Australian governments effectively manage the second and subsequent order consequences of cybersecurity incidents.

The CIMA categorises the cyber security threat environment from Levels Five to One – Five being 'Normal Conditions' and One being 'National Cyber Crisis' (Appendix D). Whilst there is no direct correlation between these levels and those used within this Plan, they may both be referred to during communications with WA State agencies to provide awareness of local incidents and the national threat environment.

The CIMA identifies the National Cyber Security Committee (NCSC) as the peak cyber security coordination body for Australian governments and provides strategic coordination of national response efforts. Its members (or their representatives) are responsible for leading their jurisdiction's response to a national cyber incident. DPC represents WA on the NCSC.

The NCSC has the authority to declare an incident or change the cyber security threat environment under the CIMA. The NCSC's role in responding to a national cyber incident includes:

- facilitating the exchange of threat intelligence and solutions to enhance jurisdictions' situational awareness and response activities;
- overseeing the development of nationally consistent public information;
- providing a forum for consultation that informs members' briefings to their respective senior stakeholders (including Ministers), and
- facilitating, where practicable, the sharing of expertise and resources to support jurisdictions' responses.

If a national cyber incident reaches crisis level, the CIMA will support jurisdictions' respective crisis management arrangements by activating the Australian Government Crisis Arrangements under the Australian Government Crisis Management Framework through the Australian Government Crisis and Recovery Committee or National Coordination Mechanism. In addition, national consequence management responses may be supported by the Australian Government's National Situation Room and led by the formation of an Australian Government Crisis Coordination Team.

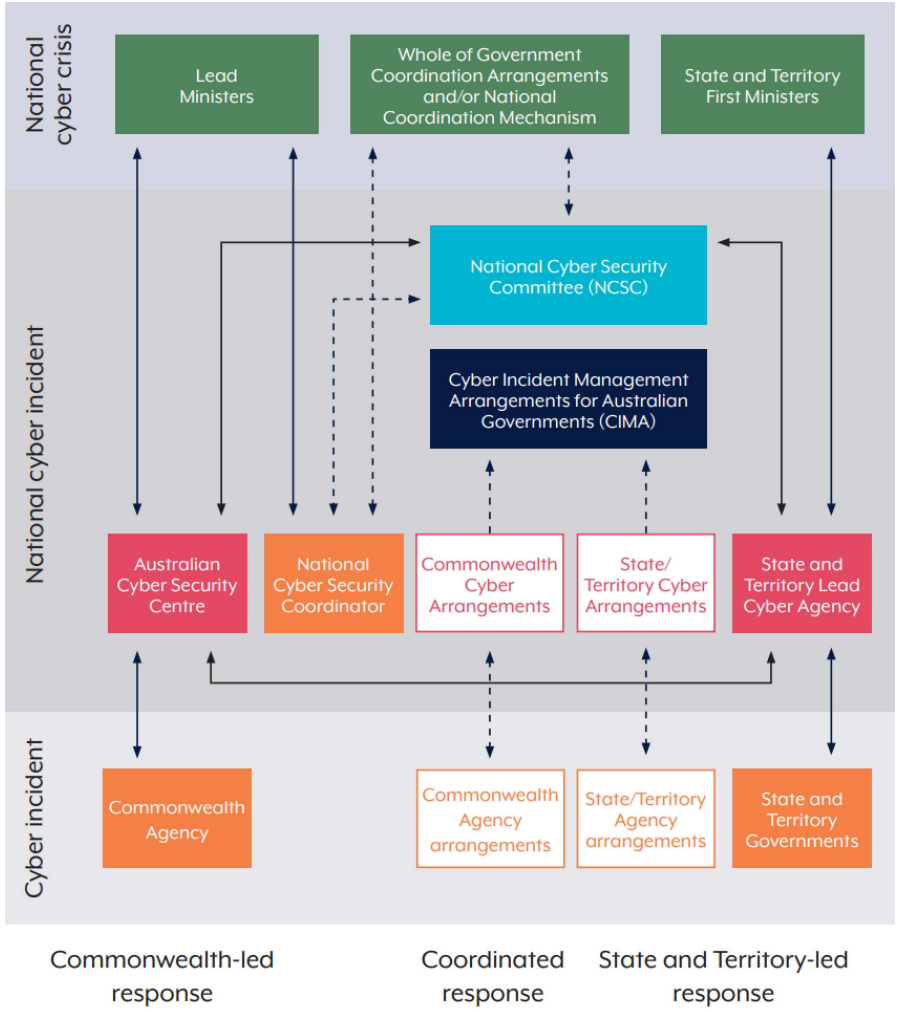


Figure 1. National coordination framework for government cyber incident management

Print on A3 to pass print accessibility.

3.4 Exercising arrangements

The arrangements will be exercised and strengthened in partnership with WA Government and Australian Government agencies , businesses and international cyber security partners. DPC, through DGov will participate in the review of exercise outcomes to inform continuous improvement of the arrangements.

WA will also participate in national exercising arrangements through the ACSC's national cyber security consequence management exercise program. The program focuses on coordinating responses to impacts on affected entities. This includes using regulatory and information-sharing frameworks to help impacted organisations to respond to cybersecurity incidents. The exercises involve:

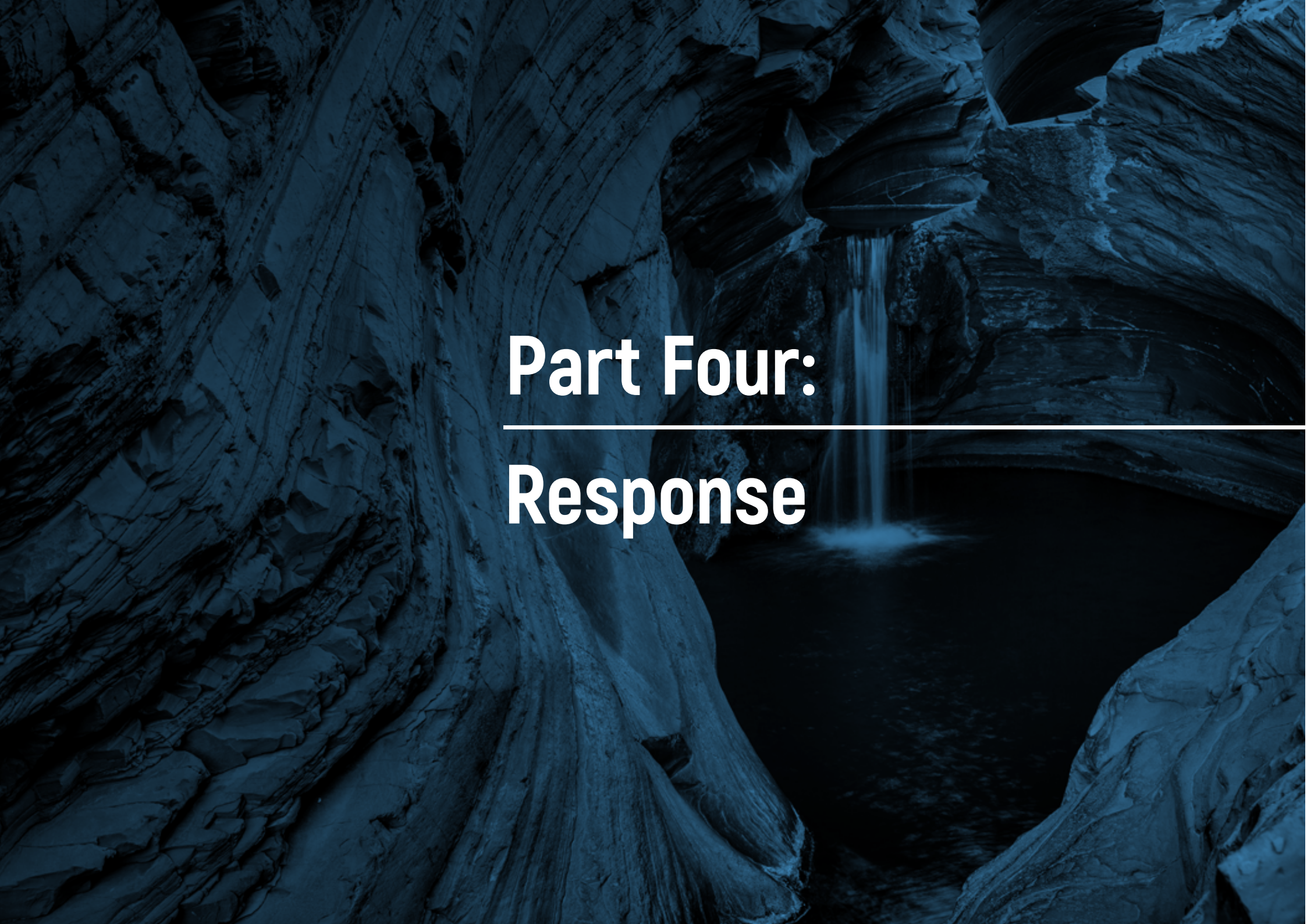
- Australian Government, state and territory cyber security agencies
- emergency management agencies
- First Minister Departments
- departments responsible for specific sectors.

3.5 Community information and education

The HMA, in collaboration with subject matter experts contributes to the development of education programs and materials to inform and educate the public, government and industry on the notification, risk and management of a cybersecurity incident.

3.6 Local Emergency Management Arrangements

Due to the nature of this hazard requiring a state level response, it is not expected that each local area will have a local cybersecurity incident response plan, however each local government should consider whether their Local Emergency Management Arrangements (LEMA) would enable an appropriate response to resulting impacts of a cybersecurity incident emergency, for example service disruptions, and have in place the resources and capabilities to respond.



Part Four:

Response

4.1 Responsibility for response

4.1.1 HMA response to a cybersecurity incident

As the HMA, DPC is responsible for the coordination and management of response activities for Cybersecurity Incidents. Response activities will be carried out in accordance with this Plan and the CIMA will be activated when a national incident is declared by the NCSC.

It may take some time before it becomes apparent that an incident is cyber related. Where the cause of an emergency is not immediately apparent, the designated HMA for the consequential emergency will lead in combatting the effects of that emergency. If the cause of the emergency is deemed to be cyber related, the HMA for cybersecurity incident will assume responsibility for, and control of, the overall management of the cybersecurity incident occurring.

Ongoing assessment of the cybersecurity incident will be undertaken as the incident evolves. Should it be determined by the HMA in consultation with the NCSC that the incident meets the CIMA threshold of NCSA-2 or below, the additional national arrangements will be activated.

4.1.2 Cyber Security Incident Coordination Framework

The CSICF outlines the process for management of cybersecurity incidents for the WA Government, from incident identification to recovery.

Accountable authorities (CEOs, Directors General or chief employees) of entities are responsible for implementing requirements of WA Government Cyber Security Policy and CSICF as they relate to response including:

- Reporting Cyber Incidents within 6 hours of their becoming aware of the incident to the Office of Digital Government (DGov)
- developing and implementing entity cybersecurity incident management/ response plans
- develop and perform annual cybersecurity exercises.

4.2 Principles

The following principles have been developed to guide decision-making in the management of cyber security incidents. The principles provide a common understanding of priorities to be considered, and how entities should cooperate with each other to maximise the effectiveness of response activities.

Principle 1: Public and individual safety is the highest priority

In managing cyber security incidents, the highest priority is public safety. When an incident involves the compromise of sensitive information or the compromise of an asset that could put public safety at risk, the response must prioritise measures to address these risks ahead of other considerations.

Principle 2: Protection of personal information

The protection of personal information, including sensitive personal and Identifiable information (PII), held by agencies is to be prioritised ahead of maintaining or restoring service availability.

Principle 3: Protection of assets and the environment

The protection of assets owned by agencies and the environment is to be prioritised over maintaining or restoring service availability.

Principle 4: Justice

Cyber security incidents that are suspected criminal acts must be investigated by law enforcement. Investigative requirements, however, need to be considered in the context of, and balanced against, the need to effectively respond to an incident and minimise consequences.

Principle 5: Whole-of-Government cooperation, coordination and continuous improvement

Incidents must be reported, with lessons learnt shared across agencies.

A cooperative and coordinated approach between agencies to cyber security incident management, including the sharing of expertise and resources where practicable, will maximise the likelihood of effective responses to and recovery from incidents.

Principle 6: Flexible and agile

Responses to cybersecurity incidents will seek to maximise effectiveness by being flexible and agile to adapt to changing and uncertain situations.

Principle 7: Accountability

Entities' cyber security incident decision-making and actions must be accountable.

4.3 Response arrangements

The HMA provides advice to support response teams and shares information on threats to enable entities to rapidly take protection measures.

WA Government entities must implement the actionable intelligence and advice provided for prevention or detection including those specified in the WA Government Cyber Security Policy.

This section details the strategic response and the control structure for managing and responding to cybersecurity incident emergencies. Table 3 describes the WA response arrangements for each cyber incident level up to and including cybersecurity incident emergencies and the roles of the HMA, Controlling Agency and affected entities.

Level	HMA/Controlling Agency	Affected Entity
Cyber Event	• DGov Cyber Security Unit (CSU) to maintain situational awareness. • Support provided from CSU as required.	• Enact incident response and business continuity arrangements (policies and plans). • Notify DGov within 6 hours of detection.
Cyber Incident	• Minor coordination between CSU and entity with provision of advice and information. • Requires a localised response, being managed by local resources with little or no external support. • Facilities for managing the response are small scale. • Provision of advice to the Minister for Innovation and the Digital Economy (if required).	• Enact incident response and business continuity arrangements (policies and plans). • Notify DGov and the ACSC of Cyber Incidents and Significant Cyber Incidents as soon as practicable. Agencies and entities captured by the *Security of Critical Infrastructure Act 2018* (SOCI Act) (Commonwealth) are required to report Cyber Incidents within the timeframes of the Act. • Support the ACSC and WA Police Force investigations into incidents.
Significant Cyber Incident	• Major CSU coordination of information requiring a local or regional response, being managed primarily at the local level, with some support being coordinated by the state. A dedicated Local Control Centre may be required to manage the response if the situation escalates. • Provision of advice to the Minister for Innovation and the Digital Economy • Implementation of arrangements established under the state emergency management legislative and policy framework.	• Notify DGov and the ACSC of Cyber Incidents and Significant Cyber Incidents as soon as practicable. Agencies and entities captured by the SOCI Act are required to report Cyber Incidents within the timeframes of the Act. • Enact Incident response, crisis management and business continuity arrangements (policies and plans). • Initiate emergency related provisions under contracts, licenses or industry specific legislation as required. • Support the ACSC and WA Police Force investigations into incidents.
Cyber Crisis	• Full control of the situation by the HMA requiring a state-wide response, being managed primarily at a state level. This may include the establishment of one or more Local Control Centres and a fully operational State Coordination Centre. Some resource support may be provided from outside the responsible agency or state. • Significant State and national coordination of information and resources. • Declaration of an Emergency Situation or State of Emergency and implementation of established arrangements. • Development and/or exercise of emergency powers and emergency regulations where appropriate.	• Enact Incident response, crisis management and business continuity arrangements (policies and plans). • Notify DGov and the ACSC of Cyber Incidents and Significant Cyber Incidents as soon as practicable. Agencies and entities captured by the SOCI Act are required to report Cyber Incidents within the timeframes of the Act. • Emergency related provisions under contracts, licenses or industry specific legislation • Support the ACSC and WA Police Force investigations into incidents.

Table 3. WA cyber incident levels and response arrangements

4.4 Notifications

Entities are required to notify DGov of suspected or confirmed cyber security incident to DGov within 6 hours of detection. Entities captured under the *Security of Critical Infrastructure Act 2018* (SOCI Act), are required to report cyber incidents within the required timeframes specified under the SOCI Act to the ACSC.

The HMA provides information to the State Emergency Coordinator (SEC) and the emergency management sector on any current actions and forecast impacts as advised by the Controlling Agency and Australian Government agencies. If the HMA and the SEC determine the incident constitutes an emergency, the State Emergency Coordination Group (SECG) may be established by the SEC on request of the HMA or on the SEC's own initiative in consultation with the HMA.

In addition to section 5.2.3 of the State EM Plan, on determination of an emergency (as above), the HMA will notify:

1. WA Government agencies as per the Response Arrangements (Table 3);
2. WA Police Force of any suspected or actual cybercrime; and
3. the ACSC.

4.5 Levels of response

The declaration of an incident level is a critical component of emergency management in terms of triggering the responsibilities and actions of emergency management agencies and to ensure a response in which the size of both the Incident Management Team and the coordination structure are proportional to the size of the cybersecurity incident.

The HMA has established different incident levels to those under the State Emergency Management Plan section 5.1.5. These incident levels, with incident indicators (descriptors), are organised in the colour-coded Alert Warning System (AWS) colours, as outlined in Table 4 of this Plan. Table 5 shows the comparison of the WA cybersecurity incident levels against the State Emergency Management incident levels and the National CIMA Levels (provided in Appendix D).

Cyber Event Level 1

Assigned to any local or limited response that has limited potential impact on government, industry, community, or the environment, and can be managed within an entity's resources. There is a low level of complexity and minimal impact on the community.

Note: A Level 1 incident in the State EM Plan equates to a Level 1 or 2 response in this plan.

Cyber Incident Level 2

Assigned to any incident that is likely to cause severe and widespread impact on government, industry, or the environment, and requiring management and coordination at a state level. There is likely to be a medium level of complexity and impact on the community. Support from an agency or agencies may be required.

There is potential for the incident to be declared a **cybersecurity incident emergency.**

Note: A Level 2 incident in the State EM Plan equates to a Level 2 or 3 response in this Plan.

Significant Cyber Incident Level 3

Assigned to any incident likely to cause catastrophic consequences for government, industry, community or environment and may potentially impact the whole of WA. A significant multi-agency response will be required. A declaration of an "Emergency Situation" or "State of Emergency" may be required.

Note: A Level 3 incident in the State EM Plan equates to a Level 3 or 4 response in this Plan.

Level	Indicators (Descriptors)
L1 Cyber Event	• Attempted compromise or cyber-attack, with no impact to systems or services, that is: – Manageable through business-as-usual operations. – Primarily address through automated security controls or limited manual intervention.
L2 Cyber Incident	• Successful compromise of individual agency security controls that requires corrective action. • Minor to moderate impact to services, information, assets, reputation or relationships and requires manual intervention from multiple persons and/or engagement with other organisations.
L3 Significant Cyber Incident	• Successful compromise of security controls that requires corrective action. • Significant to major impact to services, information, assets, government reputation, relationships and/or community. Includes an incident that involves: – more than one organisation; or – a data breach involving personal information.
L4 Cyber Crisis	• Successful compromise of security controls that: – has the potential to cause or is causing loss of life and extensive damage to property, infrastructure or the environment; and/or – has the potential to have or is having significant adverse consequences for the Western Australian community or a part of the Western Australian community.

Table 4. WA cyber incident level indicators

Overlap between incident levels

At times there will be some overlap between the indicators for the incident levels. The Operational Area Manager (OAM) will determine the incident level based on the actual and/or potential impact of the incident. Satisfying one or more of the "indicators" does not automatically necessitate an escalation to that level. The indicators in Table 4 are provided for consideration and guidance only.

State EM Incident Levels	WA Cybersecurity Incident Levels	National CIMA Levels
Level 1	Level 1 or 2	NCSA-4 or NCSA-5
Level 2	Level 2 or 3	NCSA-4 or NCSA-5
Level 3	Level 3 or 4	NCSA-1 or NCSA-2

Table 5. Incident level comparison

4.6 Activation of this plan

The response arrangements within this Plan will be activated for incidents declared a cybersecurity incident emergency by the HMA in consultation with the SEC with situational intelligence from State and national sources.

The HMA may escalate an incident declaration in response to additional threat intelligence gained from the affected agency, other agencies (including agencies from other jurisdictions) and/or in response to a change in the incident levels.

4.6.1 Declaration of Emergency Situation or State of Emergency

The HMA, or the SEC may make an 'Emergency Situation Declaration' when the situation requires the use of additional emergency powers provided under the EM Act.

The Minister responsible for the EM Act (after considering the advice of the SEC) may declare a 'State of Emergency' when the situation requires the use of additional emergency powers provided under the EM Act.

The above declarations enable authorisation of Hazard Management Officers or Authorised Officers (as applicable) who are able to exercise powers, such as directing movement and evacuation and taking control of or making use of places, vehicles or other things.

Note: Appointed Hazard Management Officers and Authorised Officers may only exercise a power under Part 6 of the EM Act subject to the terms and conditions on which they have been authorised. Refer to State EM Procedures 4.6 and 4.13 for further information.

4.7 Hazard management structure/ arrangements

The levels of coordination that shall be activated in response to an incident arising from a cybersecurity incident emergency will be in accordance with state level policies and plans and local emergency management arrangements, and, if the cybersecurity incident emergency is a (suspected) terrorist act, the State Hazard Plan - Hostile Act and the National Counter-Terrorism Plan will be enacted.

To facilitate coordination between the Incident Command and other relevant entities, the HMA or Controlling Agency may establish Incident and/or Operational Area Support Groups. An incident management structure for cybersecurity incident emergencies is illustrated in Figure 2.

An Incident Support Group, Operational Area Support Group and a SECG may be established by the SEC to facilitate the provision of coordinated emergency management by public authorities and other organisations at a strategic level, with a focus on state level impacts of the emergency.

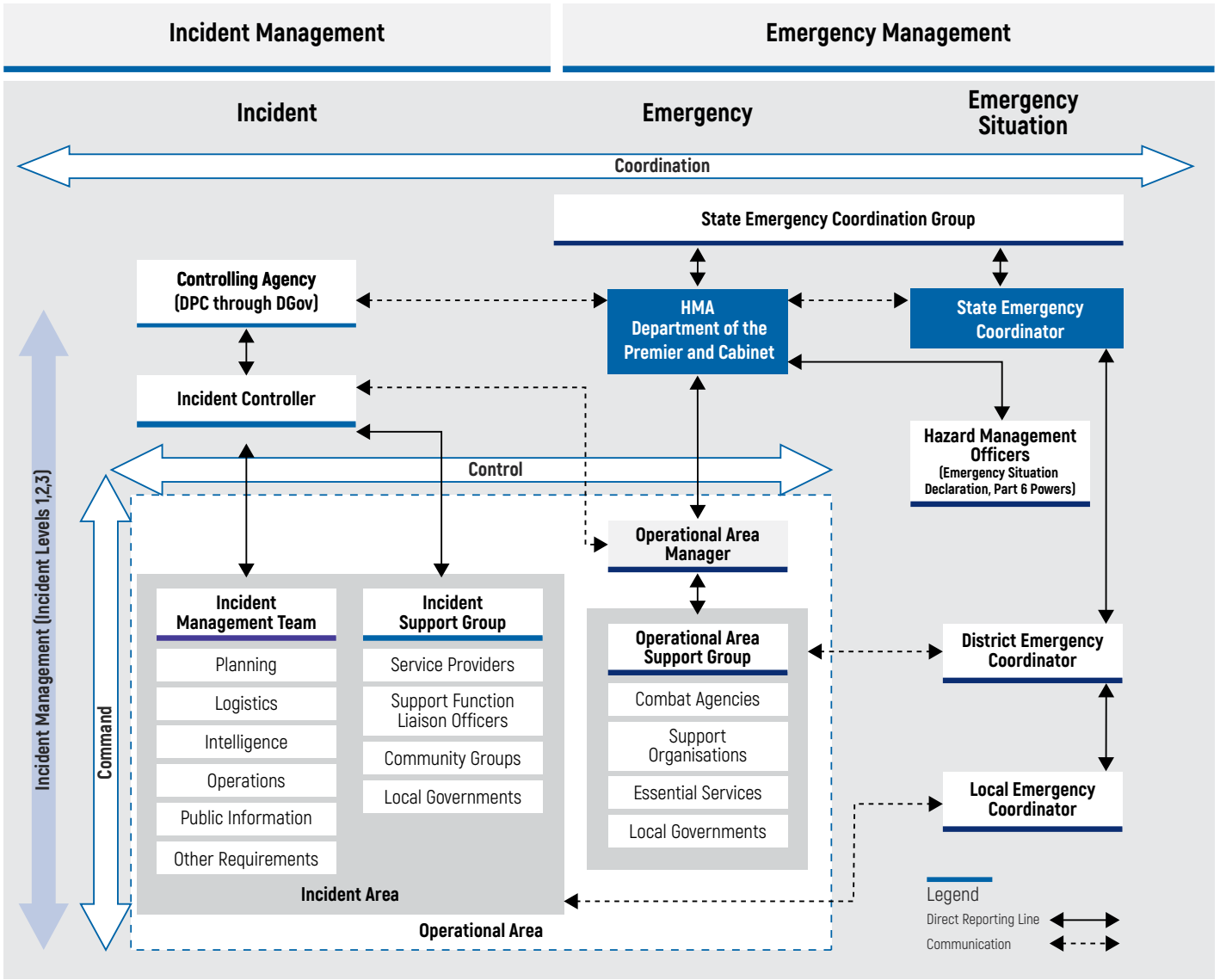


Figure 2. Incident management structure for cybersecurity incident emergencies

Print on A3 to pass print accessibility.

Further details on these arrangements and functions can be found in sections 5.1 to 5.4 of the State EM Policy and section 5 of the State EM Plan.

4.7.1 Multiple emergencies

In the event that another emergency occurs as a consequence of a cybersecurity incident, the designated HMA for the consequential emergency will be required to assist in managing the effects of that emergency. The HMA will remain responsible for, and in control of, the overall management of the cybersecurity incident.

4.7.2 Industry emergency response arrangements

Australia uses a tiered, partnership-based model for cyber incidents, where Industry remains responsible for its own response, but government coordination and assistance will scale up as impact increases.

Industry captured under the SOCI Act, are required to establish a set of incident management and business continuity arrangements. These arrangements are activated either in anticipation of an emergency, or in direct response.

4.8 Support services

There are numerous support services undertaken by relevant designated agencies. These support services, including health services and emergency relief and support, are outlined in section 5.9 of the State EM Policy, and section 5.3 of the State EM Plan. Support plans that may be activated in support of this Plan may include:

- IDCARE national identity and support for government, industry and citizens.
- State Support Plan - Emergency Public Information activated by the State Emergency Public Information Coordinator.

4.9 Public warnings/information

Intense media and public interest can be anticipated during some cybersecurity incidents. The HMA is responsible for the provision of public information and media management during a cybersecurity incident response.

In triggering this Plan, the HMA will provide community information in a coordinated manner through the Incident Controller and/or Operational Area Manager to enhance awareness and assist community members impacted by the hazard. All public statements relating to the emergency will be issued through an approved written media release, or a spokesperson officially authorised by the HMA to release such information.

Individual agencies are responsible for developing and clearing public information related to their assets and services during an incident. While individual agencies are responsible for their own public information, they must coordinate with the HMA to ensure consistency of messages across agencies.

In an incident involving inter-jurisdictional coordination, the HMA will liaise with the Australian Government and other States and Territories on public information.

The HMA will manage the provision of information to the media to meet their regular needs and ensure the provision of appropriate and timely information and instructions to government, industry, and the general public.

4.10 Stand down and debriefs

The stand down phase of the response commences when the response strategy has been effective and the hazard is under control.

The HMA will ensure the debriefing of all participating organisations and personnel involved in the emergency response within a reasonable timeframe following the response stand-down phase.

Investigations into the cybersecurity incident may continue after stand down.

4.11 Post incident review

At the completion of response operations, each agency or organisation involved in the response shall, on request from the HMA provide a written report outlining their involvement and any identified lessons, improvements, and recommendations for consideration. These reports will be collated into a post-operation report to be forwarded to the relevant Ministers and the SEMC.

The Directors General Technology, Innovation and Science Council (TISC) comprising Director Generals will consider and endorse recommendations of the review. The Business and Technology Advisory Committee (BATAC) through the Cyber Security Working Group (CSWG) will drive the recommendations across agencies to reduce impacts from the specific significant cybersecurity incident or crisis, and to inform preparation and prevention for future incidents.

Post incident analysis/review will be undertaken as per State EM Policy section 5.11, State EM Plan section 5.7 and State EM Response Procedure 4.22

Part Five:

Recovery

Recovery involves restoring or improving of livelihoods and health, as well as economic, physical, social, cultural and environmental assets, systems and activities, of a disaster-affected community or society, aligning with the principles of sustainable development and 'build back better', to avoid or reduce future disaster risk" (Australian Disaster Recovery Framework (2022)). These activities will generally commence simultaneously with the Response phase.

5.1 Responsibility for recovery

The HMA and Controlling Agency have a role in initiating both relief and recovery during Cybersecurity Emergencies. DPC, as the HMA is responsible for commencing recovery as soon as practicable during an emergency (State EM Policy statement 6.2.2).

Under this Plan, DPC through DGov will carry out the functions and the responsibilities of the Controlling Agency to gain an understanding of known or emerging recovery impacts during the response to an emergency and to coordinate the completion of an Impact Statement in accordance with State EM Plan section 6.2 and State EM Recovery Procedure 5.3. The Impact Statement will be developed in consultation with the members of the Incident Support Group, Operational Area Support Group, Local Government Recovery Coordinator/s and other relevant agencies.

It is a function of local government to manage recovery following an emergency affecting the community in its district (section 36(b) EM Act).

The extent of recovery activities will depend on the nature and magnitude of the emergency. In some circumstances, it may be necessary for the State government to assume responsibility for coordinating the recovery process at a whole-of-government level. This will be the case where a large section of the State is impacted by a disruption for an extended period of time.

Following an emergency resulting from a significant cybersecurity incident, a recovery committee may be formed for strategic coordination of recovery activities.

Each entity must incorporate recovery from cybersecurity incidents into its Business Continuity and Recovery Plan and regularly review and test it, to ensure an effective response and prompt recovery following a cybersecurity incident emergency.

WA Government Cyber Security Incident Coordination Framework

Accountable authorities (CEOs, Directors General or chief employees) of entities are responsible for implementing requirements of WA Government Cyber Security Policy and Cyber Security Incident Coordination Framework (CSICF) as they relate to recovery from impacts of a cybersecurity incident including:

- Including cyber security in business continuity planning
- Ensuring adequate cyber security insurance
- Performing post-incident review on significant incidents
- Sharing lessons learned with the rest of WA Government.

Appendices

Appendix A: Distribution list

This State Hazard Plan is available on the SEMC website. The agencies below will be notified by the HMA (unless otherwise specified) when an updated version is published on this website:

- All agencies and organisations with responsibilities under this Plan
- National Emergency Management Agency (SEMC Business Unit to notify)
- Minister for Emergency Services (SEMC Business Unit to notify)
- Minister for Science and Innovation (DPC to notify)
- State Emergency Management Committee (SEMC), subcommittee and SEMC reference group members (SEMC Business Unit to notify)
- State Library of Western Australia (SEMC Business Unit to notify).

Appendix B: Glossary of terms and acronyms

B1 Glossary of terms

Terminology used throughout this document has the meaning prescribed in section 3 of the EM Act or as defined in the State Emergency Management Glossary. In addition, the following hazard-specific definitions apply.

Term	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 as defined in the NIST Privacy Framework Version 1.00.
cybersecurity incident	An event or situation in which: (a) an electronic system is modified or impaired (b) a threat is made that causes a person to have a reasonable suspicion that an electronic system is being or will be modified or impaired (c) a person reasonably suspects that an electronic system is being or will be modified or impaired. (EM Regulations r. 14B)
emergency	as used within the term **cybersecurity incident emergency** refers to: the occurrence or imminent occurrence of a hazard which is of such a nature or magnitude that it requires a significant and coordinated response (EM Act Section 3)

Table 6. Glossary

B2 Acronyms

Term	Definition
ACSC	Australian Government's Australian Cyber Security Centre
AWS	Alert Warning System
BATAC	Business and Technology Advisory Committee through the Cyber Security Working Group (CSWG)
CEO	Chief Executive Officer
CIMA	Cyber Incident Management Arrangements for Australian Governments
CSICF	Cyber Security Incident Coordination Framework
CSU	Cyber Security Unit, DGov
CSWG	Cyber Security Working Group
DGov	Office of Digital Government, Department of the Premier and Cabinet
DPC	Department of the Premier and Cabinet
EIMS	Emergencies Incident Management System
EM Act	*Emergency Management Act 2005*
GCIO	Government Chief Information Officer

Term	Definition
GTE	Government Trading Enterprise
HMA	Hazard Management Agency
HMO	Hazard Management Officers
IoC	Indicators of compromise
IT	Information Technology
JCSC	Joint Cyber Security Centres
LEMA	Local Emergency Management Arrangements
NCSA	National Cyber Security Arrangements
NCSC	National Cyber Security Committee
OAM	Operational Area Manager
OT	Operational Technology
PSPF	Australian Government Protective Security Policy Framework
SEC	State Emergency Coordinator
SECG	State Emergency Coordination Group
SEMC	State Emergency Management Committee
SHP – Cybersecurity Incident	State Hazard Plan – Cybersecurity Incident
SIEM	Security Incident and Event Management System
SOCI Act	*Security of Critical Infrastructure Act 2018* (Commonwealth)
State EM Plan	State Emergency Management Plan
State EM Policy	State Emergency Management Policy
the Core	GovNext Core
TTP	Techniques and Procedures
WA	Western Australia

Table 7. Acronym list

Appendix C: Roles and responsibilities

Entity	Responsibilities
The Department of the Premier and Cabinet – Hazard Management Agency	Carries out the functions and responsibilities of a Hazard Management Agency (HMA) as detailed in Appendix A of the State Emergency Management Policy. The Director General of the Department of the Premier and Cabinet and Government Chief Information Officer are authorised to act in the name of the HMA in the roles and functions as prescribed in sections 50, 53, and 55(1) of the EM Act.
Department of the Premier and Cabinet through the Office of Digital Government	Carries out the functions and responsibilities of a Controlling Agency as detailed in Appendix A of the State Emergency Management Policy, and: • Notifying the Australian Government's Australian Cyber Security Centre (ACSC) of Cyber Incidents, Significant Cyber Incidents and Cyber Crises. • Coordination of State responses upon activation of the Cyber Incident Management Arrangements for Australian Governments (CIMA). • Is informed of, and communicates to affected agencies, activities undertaken by the MSPs of the GovNext Core (the Core) in response to identified vulnerabilities and/or incidents. • Instructs GovNext Core MSPs to isolate, or otherwise contain the network traffic of individual or collective agencies that would present a clear threat to other agencies connected to the Core or other external parties. This authority would be at the direction of the Government Chief Information Officer (GCIO) or DGov's Chief Information Security Officer in consultation with, where possible, affected agencies.
WA Government Chief Information Officer, Office of Digital Government	In addition to having the authorisation to act as the HMA in the roles and functions as prescribed in sections 50, 53, and 55(1) of the EM Act: • Drive cyber security and digital transformation, key priorities of the Western Australian Government Digital Strategy • Provide whole-of-government policy leadership, advice and direction on digital transformation, cyber security and incident prevention and management.
WA Police Force	• Investigates suspected technology crimes in Western Australia and supports criminal prosecutions. • Responsible for inter-jurisdictional cybercrime liaison.

Entity	Responsibilities
Accountable Authorities (CEOs, Directors General or chief employees) of entities within the scope of the WA Government Cyber Security Policy **Note:** Any entity not included in the scope of the WA Cyber Security Policy is encouraged to undertake these activities.	• Prepare for cybersecurity incidents by developing and exercising cybersecurity incident management/response plans and incorporate cyber risk in corporate business continuity and disaster recovery plans. • Manage/control its responses to cybersecurity incidents impacting its organisation in accordance with their cybersecurity incident management/response plans (including reporting to Board/Corporate Executive). • Coordination with DGov, all agencies are: – to establish and provide notification to DGov of a nominated Security Executive including email and telephone contact. – to report to DGov identified Cyber Incidents, Significant Cyber Incidents, potential Cyber Crises and significant increases in Cyber Events within 24 hours of the discovery. To maximise the benefits of a coordinated response framework, information related to the type of incident, known indicators of compromise (IoC's) and Tactics, Techniques and Procedures (TTP's), and impact to agency operations must be reported as quickly as possible. – to provide DGov with regular updates on preventative and remediation actions taken. • Coordination with the WA Police Force, all agencies will: – notify the TCS of applicable Cyber Incidents and Significant Cyber Incidents as soon as practicable. DGov can be requested to report incidents to the WA Police Force on behalf of agencies. – support the WA Police Force investigations into incidents by providing relevant data and records. • Support to other agencies: – Where practicable, support other agencies' responses to cyber incidents (e.g. through the provision of expertise and resources where appropriate). – Support operational-level coordination arrangements. – Support strategic-level coordination arrangements. – Support inter-jurisdictional coordination arrangements (e.g. through the provision of information to DGov to support the State's engagement in these arrangements). – Provide advice to their Ministers and support Ministerial coordination arrangements. – Support whole-of-government public information arrangements.

Entity	Responsibilities
Support organisations	• Responsible for specific activities in support of the Controlling Agency/HMA, and may also support Combat Agencies and other Support Organisations upon request.
RiskCover	• Provides cyber risk insurance cover and access to cyber-incident response services through their reinsurance partners AIG. • Response Management: RiskCover provides access to a cyber-incident response team comprised of industry specialists, with initial free triage and extended assistance at preferred rates. Services include: – forensic services following a data breach; – assistance to repair company and individual reputations; – breach response advisors; and – associated notification costs.
IDCare	• Incident Response Support, including: – A 24/7 Incident Response capability. – Incident Referral Code established within 24 hours – these codes allow a victim to identify themselves as being part of a particular breach, giving them access to the correct case managers/support resources. – Priority referrals and Specialist Case Management for sensitive breaches or individuals. – Referral portal for a data breach response, allowing affected agencies to see the cases managed by IDCARE.

Table 8. Response roles and responsibilities

Appendix D: CIMA National Cyber Security Arrangements (NCSA) levels

Response Level	Characteristics that inform key response activities	
5	**Normal Conditions (day to day posture in absence of activation)**	Baseline state of readiness across Australian governments. Cyber security posture, resources and arrangements are within the capability and capacity of jurisdictional responses, with no additional resources or coordination required beyond regular collaboration and intelligence sharing.
4	**Lean Forward**	Inter-jurisdictional coordination is required to manage a potential threat. Precautionary elevated monitoring, technical analysis, strategic coordination, and engagement across Australian governments.
3	**Alert**	A credible and time sensitive cyber threat or incident exists requiring incident response and preparation and response activity in more than one jurisdiction. Also requires active monitoring, analysis, and strategic planning to prevent and mitigate harm, including inter-jurisdictional coordination of technical, consequence management and public communication activities.
2	**National Cyber Incident**	Significantly impacts, or has the potential to significantly impact, multiple jurisdictions either simultaneously or through spread, and/or a coordinated inter-jurisdictional incident response is required which may include the separate activation of crisis arrangements at the national level or in an affected jurisdiction.
1	**National Cyber Crisis**	A national cyber crisis requires a collective, strategic approach to response. It has caused, is causing or has the potential to cause significant sustained disruption to the supply of essential goods and services, cause severe economic damage, threatens national security, and has, or could lead to the loss of life.

Table 9. National Cyber Security Arrangements (NCSA) levels