Australian Government
National Office of Cyber Security

Australian Cyber Response Plan (AUSCYBERPLAN)

June 2025

Version 1.0

Table of Contents

1. Introduction

1.1. Purpose

The **Australian Cyber Response Plan** (AUSCYBERPLAN) outlines the Australian Government's cyber incident response coordination arrangements to cyber incidents. It provides an overview of the Australian Government's various cyber incident response coordination arrangements, describes response activities covered by those arrangements and identifies the departments and agencies responsible for those arrangements.

AUSCYBERPLAN is the national plan for cyber incident hazards categorised as crises under the **Australian Government Crisis Management Framework** (AGCMF). The AGCMF defines cyber incidents and designates the Minister for Cyber Security as the Lead Minister, with the National Cyber Security Coordinator (the Coordinator) and the National Office of Cyber Security (NOCS) in the Department of Home Affairs as the Lead Coordinating Senior Official and the Australian Government Coordinating Agency respectively for coordinating responses to cyber incidents. AUSCYBERPLAN is also complementary to the **2023-2030 Australian Cyber Security Strategy** and the **Cyber Incident Management Arrangements** (CIMA) that outline the national technical response arrangements.

1.2. Response activities

AUSCYBERPLAN recognises that cyber incidents may require the coordination of several response activities across governments:

- **Technical response** activities focused on the cyber incident itself, including advice and assistance, incident management, information sharing and remediation.
- **Consequence management** activities focused on managing the impacts of the cyber incident, including cyber, digital and information consequences, as well as the broader consequences affecting the Australian community and/or Australian interests domestically and overseas (such as government or industry services).
- **Emergency management** or crisis management, including a range of measures to manage risks to communities and the environment, and the organisation and management of resources for dealing with all aspects of emergencies.
- **Law enforcement** activities focused on investigating criminal activity and supporting victims of crime in conjunction with other agencies.
- **Regulatory response** activities focused on ensuring the security and stability of industry sectors and protecting customers and consumers from the impacts of cyber incidents.
- **Crisis communications** which includes:
    - Public communications activities focused on supporting communication to the public about the impacts of a cyber incident. This includes public information about the impact of incidents and actions that can be taken, and government and industry actions to support responses to these incidents.
    - Cross government communications activities to ensure situational awareness across other government stakeholders, to facilitate a shared situational awareness across governments, including the provision of advice to key personnel including Ministers, cyber lead agencies in states and territories, and relevant committees as required.

- **Attribution** activities focused on deterring and responding to malicious cyber activity, including imposing costs on actors outside Australia who carry out or facilitate significant cyber security incidents when there is sufficient evidence and it is in Australia's national interest to do so.

The Australian Government's activities under AUSCYBERPLAN are conducted in partnership with **state and territory response** activities. State and territory governments often conduct parallel or equivalent activities focused on preventing or reducing the impacts of cyber incidents impacting their jurisdictions. These activities may involve national coordination across threat intelligence sharing, resources and capability, technical response, consequence management, emergency management, law enforcement, regulatory and public communications activities.

1.3. Scope

AUSCYBERPLAN is applicable for the Australian Government's crisis response to a cyber incident that both:

- meets the definition of 'cyber incident' under the AGCMF as per Section 2.1.1., regardless of the malicious intent and/or origin of the incident.
- is determined, at the Australian Government's discretion as per Section 4.2. of the AGCMF, to require Australian Government coordination.

Outside of the NOCS, the Department of Home Affairs is the Australian Government Coordinating Agency for two other identified hazards under the AGCMF which have their own national plans to outline coordination arrangements. These include the Australian Government Domestic Security Crisis Plan (AUSSECPLAN) for domestic security-related incidents (excluding terrorist incidents), and the National Counter Terrorism Plan (NCTP) for domestic terrorist incidents.

AUSCYBERPLAN is **not** an operational or tactical plan but rather it details the strategic coordination mechanisms and arrangements between the Australian Government and state and territory governments to reduce the scope, impact and severity of cyber incidents on all Australians.

AUSCYBERPLAN does **not** control or direct:

- how individual cyber incident coordination arrangements would be activated, implemented or ceased as each arrangement will have policy, governance and planning frameworks
- processes for the assessment and management of cyber incident risk, noting it is the responsibility of entities to manage their own cyber risks
- the specific operational response activities of Australian and state and territory government entities operating under the various coordination arrangements
- a standard approach for how the Coordinator and the NOCS would leverage the various coordination arrangements to manage certain types of cyber incidents or incidents impacting specific sectors
- how other non-cyber incident coordination arrangements might be activated during a wider crisis.

AUSCYBERPLAN remains the national plan to respond to a cyber incident, except where that cyber incident is identified to be a secondary event or subset of a different identified hazard. In which case and subject to agreement, the roles and responsibilities for coordinating the Australian Government response may change. For example, where a cyber incident is an outcome or subset of a broader domestic security incident, the role of Lead Coordinating Senior Official and Australian Government Coordinating Agency may shift to the Deputy Secretary responsible for National Security and Resilience and the relevant team within the Department of Home Affairs respectively.

2. Coordination arrangements

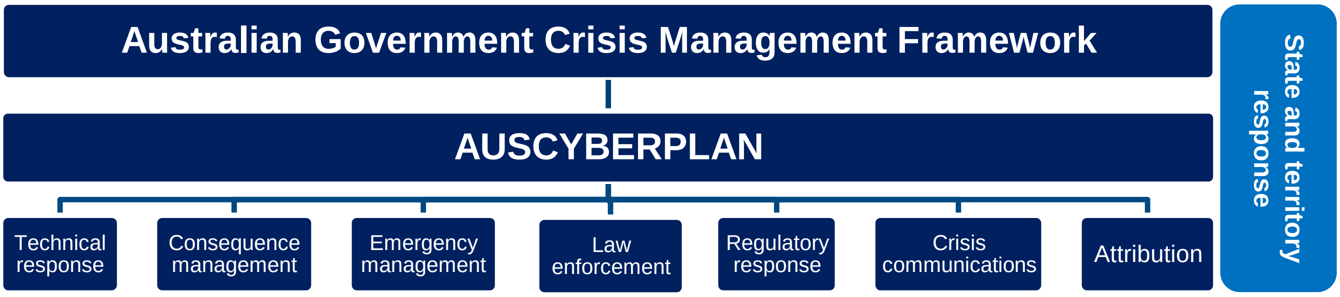

Figure 1: ***Illustrative overview of the cyber incident coordination arrangements across governments and agencies in relation to AUSCYBERPLAN***

2.1. Australian Government Crisis Management Framework

The AGCMF is the Australian Government's capstone document framing Australia's national crisis management arrangements. AUSCYBERPLAN is underpinned by the principles and administrative arrangements outlined in the AGCMF that assist Australian Government decision-makers to navigate priorities and decision-making in time-limited and challenging situations. The AGCMF manages risks holistically using an 'all hazards' approach and provides Ministers and senior officials with guidance on their respective roles and responsibilities, particularly through the accompanying Handbook to the AGCMF (the AGCMF Handbook).

2.1.1. Definition

The AGCMF defines 'cyber incidents' as follows:

> *A cyber incident is a single or series of unwanted or unexpected event(s) that have the potential to impact the confidentiality, integrity or availability of a network or system or the information that it stores, processes or communicates. This may result in significant disruption to the functioning of government or provision of government services; critical infrastructure or the provision of essential services; or may require a coordinated national response. This may include unauthorised or malicious sharing of data, manipulation or destruction of critical data and software, disruptions to ICT networks or systems, and exploitation of networks to cause a physical effect. A response to a cyber incident may require coordination under the Framework as a result of the technical considerations of the event, such as those detailed under the CIMA, or following consideration of the broader consequences of the cyber incident.*

Under the AGCMF the Coordinator, as the Lead Coordinating Senior Official, leads the Australian Government's coordination response to manage consequences to cyber incidents. The Coordinator is supported by the NOCS, as the Australian Government Coordinating Agency, and also leads whole-of-government cyber security incident preparedness efforts.

2.1.2. Mechanisms

Key mechanisms under the AGCMF that could be leveraged to respond to cyber incidents include the:

- **National Coordination Mechanism** (NCM), which provides the convening mechanism to bring together Australian Government, state and territory government, and non-government representatives during crisis coordination. The NCM is flexible, scalable and vector-agnostic.
    - It facilitates rapid problem definition and shared situational awareness, and ensures ownership of solutions to drive the rapid stabilisation of crisis events. It uses a domain or sector-based approach to promote collaboration between stakeholders with equities in the crisis, strengthening and formalising the existing relationships between governments, industry and civil society. During concurrent, compounding or complex crises, the NCM allows the harnessing of collective national capabilities to support communities.
- **Inter-Departmental Emergency Taskforce** (IDETF), which manages the whole-of-government response to overseas incidents or crises that impact, or threaten to impact, Australians or Australia's interests overseas.

Cyber incidents may also be reported to the National Security Committee of Cabinet (NSC), or another Committee of Cabinet, to inform ministerial-decision making in relation to them.

Additional coordination mechanisms which may be leveraged by the Australian Government in response to cyber incidents are outlined in the arrangements in Section 2.2.

2.1.3. Categorisation of coordination response

The AGCMF outlines triggers to activate Australian Government crisis coordination arrangements and a 4-tiered approach to guide and support appropriate and consistent levels of coordination in response to crises. As such, the severity and complexity of a cyber incident will guide the determination of appropriate coordination efforts to be provided by the NOCS and other responding agencies and departments.

The AGCMF Handbook provides general indicators in assessing crisis events to support decision making about the tier of crisis coordination, which will be considered alongside a series of internal and external factors identified by the NOCS. This may include consideration to:

- potential flow-on impacts to and interdependencies with other jurisdictions or sectors (including those identified under the *Security of Critical Infrastructure Act 2018* (SOCI Act)
- implications to international and domestic supply chains
- exposure of personal, sensitive and/or financial information
- potential impacts to the Australian Government and state and territory governments, such as the exposure of government information
- disruptions to the availability of systems and services on which Australians rely
- any other factor considered to be relevant in the determination of the appropriate level of coordination for a cyber incident.

An overview of coordination support provided by the NOCS in accordance to the AGCMF tiers of crisis coordination outlined in Figure 2, with tiers to ensure scalability and flexibility of the response given cyber incidents can evolve in scope, nature and impact. Higher tiers of coordination will require greater resourcing and cadence towards coordination and consequence management activities.

Tier 1: Coordination for an Incident Limited impact / low capacity	**May benefit from Coordinator and NOCS support** Cyber incident coordination at Tier 1 may require coordinated consequence management and response but not national or extensive multi-jurisdictional engagement. The coordination for these incidents are typically led by the impacted entity, a sector lead from an Australian Government agency, or a state or territory government. The Coordinator and NOCS may become involved if it is determined there is benefit from a degree of coordination or initial support at an Australian Government level. Cyber incidents occurring within a particular state or territory jurisdiction should continue to follow jurisdictional cyber and emergency management arrangements, with the understanding that the NOCS can support at a strategic level by leveraging the role of the Coordinator as required. The Coordinator and NOCS may monitor cyber incidents to maintain visibility, engaging with relevant stakeholders such as state and territory CISOs either directly or through mechanisms such as the National Cyber Security Committee (NCSC) to provide any support as required. Coordination mechanisms for a Tier 1 incident may include NOCS or sector-specific mechanisms from the Australian Government.
Tier 2: Coordination for a Significant Incident Major impact / moderate complexity	**May require NOCS coordination, and may also require Coordinator leadership** Significant incidents require the NOCS to take a leading coordination and consequence management role where there are meaningful benefits to a coordinated approach at the Australian Government level. In some circumstances, this might also require leadership from the Coordinator. The incident may have impacts to at least one critical infrastructure or government asset, or expose high volumes of sensitive data. It may also have the potential to cause harm or disruption to Australians. Support provided from the Australian Government is delivered in consultation with the impacted entity, relevant Australian Government agencies, and state and territory governments. Coordination mechanisms for a Tier 2 incident may include NOCS coordination, Coordinator leadership, sector-specific mechanisms, interdepartmental committees, NCM or IDETF meetings.
Tier 3: Coordination for a Nationally Significant Incident Severe impact / high complexity	**Requires Ministerial or Coordinator leadership and NOCS coordination** Nationally significant incidents require the Coordinator and the NOCS to lead the coordination and consequence management at the Australian Government level. The incident is likely to have widespread impacts on critical infrastructure or government assets, or expose very high volumes of majorly sensitive data. It also will likely have impacts across multiple sectors or jurisdictions and cause significant harm or disruption to Australians. The NOCS will support the Coordinator to activate consequence management activities, including co-chairing NCM meetings as required. The states and territories or industry may request that an NCM is activated for a specific purpose or issue. The Minister for Cyber Security will provide ministerial leadership, guidance and decision-making regarding the Australian Government response. Coordination mechanisms for a Tier 3 incident may include NCM meetings, IDETF meetings, reporting to the NSC, in addition to NOCS or sector-specific mechanisms and interdepartmental committees.

Tier 4: Coordination for a Nationally Catastrophic Incident Extreme to catastrophic impact / extreme complexity	**Requires Prime Ministerial leadership and National Emergency Management Agency (NEMA) coordination** Nationally catastrophic incidents are likely to be highly complex, have wide-ranging significant harmful impacts and consequences across multiple jurisdictions, critical infrastructure assets, government assets and data, and overwhelm Australia's systems and resources. This kind of incident is anticipated to involve most or all Australian Government portfolios. The Minister for Cyber Security, the Coordinator and the NOCS will support the Prime Minister (or delegate) and NEMA to coordinate and manage consequences relating to the cyber elements of the incident, including co-chairing cyber sector-specific NCM meetings. Coordination mechanisms for a Tier 4 incident may include NCM meetings, reporting to the NSC, IDETF meetings, in addition to NOCS or sector-specific mechanisms and interdepartmental committees. At Tier 4, the IDETF reports to the NCM.

Figure 2: Tiered coordination support provided by the NOCS for cyber incidents

2.2. Coordination arrangements for response activities

There are several Australian Government and national arrangements that may be used to coordinate the response to cyber incidents. Each of these arrangements guide how response activities should be coordinated and outline the roles and responsibilities of relevant departments and agencies. Some of these response arrangements closely align with other arrangements, and some are sector-specific and might apply to all hazards or just cyber hazards.

2.2.1. Technical response

The **Cyber Incident Management Arrangements** (CIMA) is the national technical response arrangement. It provides Australian and state and territory governments with guidance on how to collaborate technical activities in response to, and reduce the harm associated with, national cyber security incidents. The CIMA is not an operational incident management protocol. It outlines the inter-jurisdictional coordination arrangements, roles and responsibilities, and principles for the Australian Government's cooperation with states and territories in technical response to national cyber security incidents.

The CIMA is endorsed by the First Secretaries Committee and implemented by the National Cyber Security Committee (NCSC). The Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) is the lead agency on national cyber security operational matters. State and territory governments assess reported cyber security incidents considering the scope, impact and severity of an incident and its potential to harm Australia or relevant jurisdictions. If an incident meets thresholds, ASD's ACSC may declare a national cyber security incident in consultation with the NCSC members. If a national cyber security incident occurs, the CIMA will support jurisdictions respective crisis management arrangements under the AGCMF should this be required.

The **National Cyber Security Committee** (NCSC) is the peak cyber security body for inter-jurisdictional coordination and strategic oversight of technical responses to cyber security incidents. The NCSC is co-chaired by the ASD's ACSC and a state or territory government representative, and is supported by Operational, Policy, and Communications and Awareness Sub-Committees.

The NCSC includes state and territory Chief Information Security Officers (or similar) representatives, the Coordinator, the Department of Home Affairs (Home Affairs), National Emergency Management Agency (NEMA), the Australian Federal Police (AFP) and the Department of the Prime Minister and Cabinet (PM&C).

The NCSC activates the CIMA and directs the technical response activities and coordination undertaken to remediate a cyber security incident and mitigate the threat to other Australian entities.

Several sectors also have sector-specific technical response arrangements. These arrangements guide government and industry collaboration in response to security or systemic issues, including cyber incidents.

2.2.2. Consequence management

As per the AGCMF, the Coordinator and the NOCS will coordinate the Australian Government's response to cyber incidents with consequences to impact the confidentiality, integrity or availability of a network or system or the information that it stores, processes or communicates. This may include incidents which disrupt government services, critical infrastructure and delivery of essential goods and services. The Coordinator and the NOCS will manage the consequences of cyber incidents leading Australian Government coordination efforts, leveraging coordination arrangements and by standing up working groups with relevant stakeholders across governments or industry to drive specific lines of effort.

Government-industry working groups may be convened as alternatives or to complement broader mechanisms such as NCMs, depending on the tier of crisis coordination required. Incident-specific working groups may be stood up to consider issues such as government activities, industry activities, electronic discovery, identity security and services, and communications.

States and territories have the primary responsibility for consequence management within their own jurisdictions. Their activities may be supported through Australian Government coordination arrangements.

Throughout consequence management activities and the coordination process outlined in Section 4, the Coordinator and the NOCS will consider the needs of vulnerable groups who may be disproportionately at risk of harm. This may include ensuring support resources are available, accessible and bespoke for these groups to protect their cyber security, or to assist them following an incident. These groups disproportionately at risk may include, but are not limited to:

- People with disability
- People who are homeless or at risk of homelessness
- First Nations communities
- Refugee and migrant populations
- International students
- People experiencing or at risk of gender-based violence
- People over the age of 65
- Children and young people
- Lesbian, gay bisexual, transgender, queer, intersex, asexual and other non-binary, non-cisgender (LGBTQIA+) people
- Culturally and Linguistically diverse communities.

2.2.3. Emergency management

The **Australian Government Disaster Response Plan** (COMDISPLAN) is the Australian Government's all hazards emergency response plan. COMDISPLAN enables states and territories to request non-financial assistance from the Australian Government. For a jurisdiction to make a request under COMDISPLAN, one of the following criteria must be met:

- All government, community and commercial resources are exhausted or likely to be exhausted.
- The jurisdiction is unable to mobilise its own resources (or community and commercial resources) in time.

- The Australian Government has a capability that the state or territory does not have.

The Deputy Coordinator-General of Emergency Management and Response Group at NEMA activates COMDISPLAN and the Minister for Emergency Management approves any requests for assistance.

2.2.4. Law enforcement

The **Australia and New Zealand Policing Advisory Agency's (ANZPAA) Protocol for Responding to and Managing Cybercrime** (the Protocol) is the national law enforcement co-ordination arrangement. It provides guidance on the responsibilities for law enforcement agencies in responding to cyber incidents. Under the Protocol, the law enforcement agency in the geographical location of the victim is the jurisdiction responsible for responding to and managing the investigation. The intent of this approach is to enhance outcomes for victims and respond to cybercrime through prevention, disruption, deterrence and prosecution.

The AFP is responsible for cybercrime offences that target Australian Government departments, critical infrastructure, nationally significant information systems and/or data holdings, or might impact the whole of the Australian economy.

The Protocol is an internal document for police agencies and is not publicly available.

2.2.5. Regulatory response

The Australian Government has regulatory authority for the security of assets within certain critical infrastructure sectors. Several sectors have specific regulatory planning and response arrangements.

The **Cyber Security Regulator Network** (CSRN) is a forum for Australian Government regulatory authorities to consider issues relating to responding to cyber security incidents. State and territory regulators also have responsibilities for certain critical infrastructure and other essential services in their jurisdiction. This includes regulatory activities focused on ensuring the security and stability of industry sectors and protecting customers and consumers from the impacts of cyber incidents.

2.2.6. Crisis communications

The Prime Minister, the Minister for Cyber Security or their delegate may be the lead Australian Government spokesperson for cyber incidents. The Coordinator supports them to perform their spokesperson functions and may also be a spokesperson for the Australian Government, where required.

The Australian Government Crisis Communication Guidelines (AGCCG) assist the Australian Government to operationalise a coordinated and consistent public communication response to cyber incidents. This response will ensure the public is kept informed about the consequences of the incident, what the government is doing to assist and what they need to do.

As per the AGCCG, the NOCS will establish a Crisis Communication Cell for cyber incidents that will adjust in scale depending on the severity of the incident. The Crisis Communication Cell will:

- develop, in consultation with relevant government stakeholders including Sector Lead Agencies and/or Enabling Agencies, a whole-of-Australian Government crisis communications plans or strategy
- coordinate public information, in consultation with key Australian Government agencies, state and territory governments and impacted entities
- support Australian Government spokespeople with their communications requirements
- convene the Cyber Incident Communications Group, as required
- brief the NCM on communications actions underway
- adjust the communications as the cyber incident evolves.

Individual departments and agencies are responsible for communicating about incidents impacting their systems or their delivery of government services. Where a coordinated public information response is required, affected agency information will be captured in the coordinated response.

The Communication Cell will also maintain lines of communication with states and territories affected by the cyber incident through members of the Cyber Incident Communications Group, to ensure national consistency of information and messaging as the incident evolves.

2.2.7. Attribution

As outlined in the 2023-2030 Australian Cyber Security Strategy, the Australian Government undertakes attribution activities to deter and respond to malicious cyber activity, including by imposing costs on those who carry out or facilitate significant cyber incidents when there is sufficient evidence and it is in Australia's national interest to do so. This can include attributions of malicious cyber activity to cyber actors through public statements or technical advisories, or the imposition of sanctions against individuals when appropriate.

2.3. State and territory government response

The Australian Government's response to a cyber incident occurs in partnership with state and territory responses. While there are national arrangements for managing cyber incidents, state and territories often operate parallel or complementary activities.

As per the AGCMF, states and territories are the first responders to any incident that occurs within their jurisdiction and have the primary responsibility for the protection of life, property and the environment within the bounds of their jurisdiction. As such, each state and territory has responsibility for preparing for, responding to and recovering from cyber incidents and incidents which may impact their jurisdiction.

State and territory response activities are outlined in the CIMA and other jurisdictional frameworks. These reflect the machinery of government in each jurisdiction noting that not every cyber event will meet the threshold requiring escalation to a national response. These arrangements include a range of cyber-specific incident, hazard or emergency management plans or sub-plans including the need to work closely with the relevant Australian Government entities. State and territory response activities also complement or can comprise part of the national technical response, consequence management, emergency management, law enforcement, regulatory and public communications frameworks.

The Coordinator and the NOCS will engage with states and territories when relevant equities are identified.

Where states and territories are the primary lead in a response, the Coordinator and the NOCS, or ASD's ACSC, will engage with the jurisdictional lead to facilitate the provision of Australian Government support as required. This may include technical assistance and the coordination of public messaging where an incident has implications for national security. This engagement will be undertaken through state and territory cyber hazard, technical response or consequence management leads as required.

3. Roles and responsibilities

The AGCMF outlines the definition and designation of Australian Government ministers and senior officials in a crisis for identified hazards, including cyber incidents. These include a **Lead Minister**, **Australian Government Coordinating Agency**, **Lead Coordinating Senior Official**, **Sector Lead Agency** and **Enabling Agency**.

Role	Designated Official / Agency for a Cyber Incident
Lead Minister – The Australian Government minister responsible for leading coordination in response to a significant crisis caused by an identified hazard under the AGCMF.	The Minister for Cyber Security*
Australian Government Coordinating Agency – The agency required to lead the coordination across the Australian Government for a significant crisis caused by an identified hazard under the AGCMF. This agency also leads the consequence management activities within its agency functions and sector-specific responsibilities.	The Department of Home Affairs' National Office of Cyber Security (NOCS)*
Lead Coordinating Senior Official – The designated senior official within an Australian Government Coordinating Agency who is responsible for leading the coordination for a significant crisis.	The National Cyber Security Coordinator (the Coordinator) or other relevant Deputy Secretary, Department of Home Affairs*
Sector Lead Agency – An Australian Government agency that contributes to whole of Australian Government crisis coordination activities and leads the consequence management activities relevant to agency functions and sector-specific responsibilities.	Dependent on the sector(s) impacted by the cyber incident (e.g. Department of Health and Aged Care for an incident impacting the healthcare and medical sector, or the Department of the Treasury for an incident impacting the financial services and markets sector)
Enabling Agency – An Australian Government agency that administers relevant programs, provides specialist technical, scientific, intelligence or information capabilities or conducts any other enabling activities to support consequence management activities.	Key agencies include: • The Australian Signals Directorate for technical incident response arrangements • The Australian Federal Police for investigations and law enforcement response arrangements • The National Emergency Management Agency for crisis response and recovery efforts for all hazards. Other agencies and capabilities across the Australian Government may support individual incidents as required.

**For a crisis requiring Tier 4 coordination, the Lead Minister, Australian Government Coordinating Agency and Lead Coordinating Senior Official become the Prime Minister, NEMA and Deputy Coordinator-General, Emergency Management and Response, NEMA respectively.*

Figure 3: Australian Government roles to coordinate the response to a cyber incident

3.1. The Lead Minister: The Minister for Cyber Security

The Minister for Cyber Security leads Australian Government coordination of national cyber policy, responses to cyber incidents, cyber incident preparedness efforts, and strengthening of Commonwealth cyber security capability.

The Minister for Cyber Security has the following key responsibilities during a cyber incident, alongside other responsibilities outlined in the AGCMF:

- Oversees the coordinated Australian Government response to the cyber incident, including to the consequences of the incident.
- Works closely with the Minister responsible for Emergency Management, and other relevant Ministers across jurisdictions, in managing the broader consequences of the incident.
    - This may include working with impacted portfolio minster(s), or departments and agencies with independent operational requirements in the response to cyber incidents, such as lead technical response or law enforcement agencies.
- Provides advice to the Prime Minister and the NSC on whole of Australian Government priorities and consequence management objectives of the Australian Government response to the cyber incident.
- Represents the Australian Government as the principal public spokesperson at the Ministerial level on the cyber incident, in alignment with a whole of Australian Government communications strategy.

The Prime Minister is the Lead Minister for any cyber incident requiring a Tier 4 level of crisis coordination, or may delegate the Lead Minister role to the Minister for Cyber Security or another relevant minister. The Prime Minister may also decide to become a Lead Minister at their discretion.

3.2. The Lead Coordinating Senior Official: The National Cyber Security Coordinator

As the Lead Coordinating Senior Official for cyber incidents as per the AGCMF, the role of the Coordinator includes leading across the whole of Government the coordination and triaging of action in response to significant cyber security incidents and informing and advising the Minister for Cyber Security on the whole of Government response, while preserving the operational independence and role of governments and government agencies as they respond to cyber incidents.[1] By exception, a Deputy Secretary responsible within the Department of Home Affairs responsible for cyber security or critical infrastructure security may undertake the Lead Coordinating Senior Official role.

The Coordinator has the following key responsibilities during a cyber incident, alongside other responsibilities outlined in the AGCMF:

- Assesses, establishes, reviews and adapts the tier of crisis coordination required by the Australian Government to respond to the cyber incident, in consultation with key government stakeholders and in alignment with existing frameworks.
- Coordinates and triages the Australian Government's response to significant cyber security incidents, including by **facilitating** shared situational awareness across government and industry stakeholders, determining Australian Government coordination priorities and consequence management objectives, and enabling cross-government collaboration in the response.

[1] The role of the Cyber Security Coordinator is legislated through the *Cyber Security Act 2024*.

- Ensures that relevant coordination arrangements are activated and relevant response activities under those arrangements are coordinated and aligned.
- Works with NEMA to convene and co-chair the NCM as required.
- Informs and advises the Minister for Cyber Security, Prime Minister and other relevant senior decision makers to enable their leadership roles and report on actions being undertaken to respond to an incident.
- Briefs Australian Government committees, such as the NSC or interdepartmental committees, on the Australian Government's coordinated response to a cyber incident.
- Engages with impacted entities to understand how the Australian Government can support them to respond to the incident.
- Leads the development and implementation of the crisis communications strategy, supported by the Crisis Communication Cell.
- Acts as a key Australian Government spokesperson on the cyber incident, in alignment with a crisis communications strategy.
- Liaises with state and territory cyber response lead agencies through the NCSC and other forums as appropriate.
- Ensures the transfer of ongoing responsibilities and processes to relevant government stakeholders when the Australian Government coordinated response concludes.
- Leads post-incident evaluations of Australian Government coordination and consequence management activities to identify and integrate lessons learned to improve Australian Government cyber incident response arrangements.

The Coordinator **does not** use regulatory powers and cannot enforce legislative directions on an entity. This enables open coordination and collaboration with an impacted entity during a cyber incident.

The *Cyber Security Act 2024* also establishes a limited use obligation on the Coordinator that restricts how they use and share information voluntarily provided to them by industry during a cyber incident. The limited use provisions operate to ensure that information provided by industry during a cyber security incident, can only be used by government agencies (including ASD and the Coordinator), for permitted cyber purposes specified in the Act.

The Coordinator **will not** direct the operational or tactical activities of individual departments, agencies, or entities. The Coordinator's engagement with key departments and agencies may be agreed through operational protocols. These protocols would outline how the Coordinator is briefed on incidents and operational activities, coordinates certain activities, and uses and shares information received during an incident.

If the cyber incident is or escalates to a crisis requiring Tier 4 coordination, the Deputy Coordinator-General, Emergency Management and Response, NEMA becomes the Lead Coordinating Senior Official.

3.3. The Australian Government Coordinating Agency: The National Office of Cyber Security

The NOCS is housed within Home Affairs and, as the Australian Government Coordinating Agency, supports the Coordinator to perform their functions as the Lead Coordinating Senior Official. The NOCS includes a Deputy National Cyber Security Coordinator, office staff responsible for coordination activities, and seconded liaison officers from Australian Government departments and agencies.

The NOCS may engage with operational capabilities across the Australian Government such as the National Situation Room (NSR), NCM and the Australian Government Joint Crisis Coordination Team (CCT) led by NEMA.

The NOCS has the following key responsibilities during a cyber incident, alongside other responsibilities outlined in the AGCMF:

- Advises the Coordinator to inform their assessment of whether a cyber incident requires a coordinated response and at what tier.
- Engages with impacted entities to understand the nature of cyber incidents and any requirements for coordinating the government response and any public communications, in consultation with other Australian, state and territory government agencies.
- Liaises across Australian and state and territory government cyber leads and relevant departments and agencies on cyber incidents and response activities.
- Convenes coordination meetings with relevant stakeholders, including working groups, interdepartmental committees or the NCM in consultation with NEMA, to drive and coordinate lines of effort.
- Activates a Crisis Communication Cell that develops and coordinates the whole of Australian Government crisis communications strategy, distributes public information products including Holding Lines and whole-of-government Talking Points, and provides media support to the Coordinator and/or Minister for Cyber Security to enable their roles as spokespeople.
- Supports the transfer of ongoing responsibilities and processes to relevant government stakeholders when the Australian Government coordinated response concludes.
- Supports the Coordinator in conducting post-incident evaluations of Australian Government coordination and consequence management activities to identify and integrate lessons learned to improve Australian Government cyber incident response arrangements.

If the incident is or escalates to a crisis requiring Tier 4 coordination, NEMA becomes the Australian Government Coordinating Agency.

3.4. Sector Lead Agencies

A cyber incident may impact a single sector or multiple sectors. A Sector Lead Agency is an Australian Government agency that contributes to the whole of Australian Government cyber incident coordination activities. Key responsibilities of a Sector Lead Agency should align with relevant departments and agencies, in consideration to their functions and sector-specific responsibilities.

These may be agencies who are responsible for developing, maintaining, exercising and activating certain sector-specific cyber incident response arrangements. They can lead the consequence management activities relevant to their agency functions and sector-specific responsibilities as outlined in the AGCMF.

The Coordinator and the NOCS invites Sector Lead Agencies to take an active role in the broader Australian Government coordination and consequence management arrangements, as determined by the nature, extent and scope of the incident. This includes contributing to the crisis communications strategy and related products.

Individual departments and agencies are responsible for communicating about incidents impacting their systems or their delivery of government services.

3.5. Enabling Agencies

An Enabling Agency is an Australian Government agency that administers relevant programs, provides specialist technical, scientific, intelligence or information capabilities or conducts any other enabling activities to support consequence management activities.

For a cyber incident, various Australian Government departments and agencies are responsible for developing, maintaining, exercising and activating certain sector-specific cyber incident response arrangements relating to AUSCYBERPLAN:

- The **Department of the Prime Minister and Cabinet** is responsible for the AGCMF and the AGCMF Handbook.
- The **Department of Home Affairs**, outside of the NOCS, is responsible for:
    - The SOCI Act. Under the SOCI Act, this may include:
        - the application of Enhanced Cyber Security Obligations for entities designated as Systems of National Significance, as defined under the SOCI Act.
        - the use of Government Assistance Measures, designed to aid the response to serious cyber security threats or attacks.
        - ensuring compliance by specified responsible entities to develop and maintain a Critical Infrastructure Risk Management Program for their critical infrastructure assets.
        - ensuring compliance by critical infrastructure entities with the obligation to report cyber incidents which impact the delivery of essential services to the ASD's ACSC.
    - The *National Emergency Declaration Act 2020*.
        - Where a national emergency declaration is in force, the Government is able to use alternative or streamlined tests to exercise certain Commonwealth powers quickly, and cut red tape requirements in existing laws to expedite the government's response to all-hazard crises.
    - The *Cyber Security Act 2024* which introduced:
        - a 'limited use' obligation that restricts how cyber security information voluntarily provided to the Coordinator can be used and disclosed; and
        - the establishment of a Cyber Incident Review Board to conduct post-incident reviews into significant cyber security incidents.
- The **Australian Signals Directorate** is responsible for technical incident response arrangements, cyber security advice and assistance and maintains the national cyber threat picture. ASD is the Australian Government's lead representative and co-Chair of the NCSC, which has responsibility for updating and implementing the CIMA.
    - The *Intelligence Services and Other Legislation Amendment* to the *Intelligence Services Act 2024* legislates a 'limited use' obligation for ASD, similar to the 'limited use' obligation imposed on the Coordinator under the *Cyber Security Act 2024*.
- The **Australian Federal Police** are responsible for the investigation of cybercrime offences against the Australian Government, critical infrastructure, systems of national significance, and those that impact the whole of the Australian economy. The AFP are the Australian Government's lead representative member of the ANZPAA, which has responsibility for the ANZPAA Protocol.

- The **National Emergency Management Agency** supports Australian Government Coordinating Agencies by providing key Australian Government capabilities, including the Australian Government's NSR, NCM, CCT, National Joint Common Operating Picture (NJCOP), and provision of crisis planning through the Crisis Appreciation and Strategic Planning (CASP) methodology. NEMA also manages requests from states and territories for non-financial assistance through COMDISPLAN.
- The **Department of Foreign Affairs and Trade** is responsible for the foreign policy or international dimensions of the Government's response, passport, and consular services.
- The **Department of Defence** is responsible for cyber security and cyber operations on Defence networks, including Australian Defence Force warfighting networks.

Similarly to Sector Lead Agencies, Enabling Agencies may also contribute to the crisis communications strategy or related products for specific cyber incidents. Individual departments and agencies are responsible for communicating about incidents impacting their systems or their delivery of government services.

3.6. State and territory government bodies

States and territories are responsible for cyber incident response activities within their own jurisdiction. Additionally, they may operationalise parallel response activities for incidents of national significance or interest by coordinating consequence management or incident response activities within their jurisdictions and representing their jurisdictions on national working groups.

- **States and territory government bodies** are responsible for developing, implementing, maintaining, and exercising cyber-specific emergency and incident management plans. The plans should cover the state or territory's arrangements relating to all aspects of the response for each of the respective jurisdictions:
    - Technical response
    - Consequence management
    - Emergency management
    - Law enforcement
    - Regulation
    - Public communications.

States and territories may also leverage the NCSC in their response activities. The NCSC is co-chaired by a state or territory representative 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. They also, where practicable, share expertise and resources to support jurisdictions' preparedness, capability and response, as per the principles of the CIMA.

3.7. Private entities

Private entities will typically have their own cyber incident response arrangements for an incident which impacts them, including to:

- mitigate impacts on their systems
- enact business continuity measures to ensure goods and services can continue to be delivered
- release public communications
- address financial impacts
- meet any legal and regulatory obligations.

Where a cyber incident impacts private entities, those entities have the ultimate responsibility over their organisation's response to that incident. However, private entities are encouraged to cooperate with the Australian Government and relevant state and territory governments to minimise any resulting harms from cyber security incidents.

The Coordinator and NOCS will maintain situational awareness of existing response activities and provide the appropriate support from the Australian Government as outlined across the tiers in Figure 2, in consultation with the impacted entities.

Refer **Appendix B** for advice on how private entities can report a cyber incident to the Australian Government and seek support.

4. Coordination process for Australian Government response

When coordinating the Australian Government response to a cyber incident, the Coordinator as the Lead Coordinating Senior Official may undertake the following process in alignment with the crisis coordination phases of the Australian Government Crisis Management Continuum.

The response to every cyber incident will vary and these steps are not prescriptive.

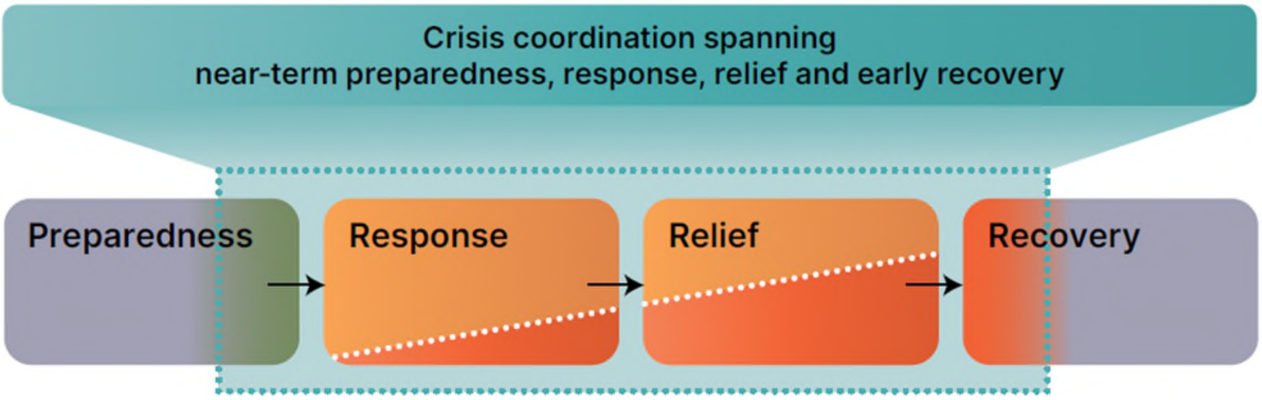
Crisis coordination spanning
near-term preparedness, response, relief and early recovery
Preparedness
Response
Relief
Recovery

Figure 4: Crisis coordination phases of the Australian Government Crisis Management Continuum

4.1. Preparedness

The Coordinator and the NOCS have established arrangements and are continuously building on them to prepare the Australian Government and the nation to respond to cyber security incidents. These include:

- ensuring the NOCS is well-equipped with an appropriate workforce and capabilities to support impacted entities by coordinating whole-of-government incident response efforts, including maintaining a crisis communications capability.
- uplifting the national cyber security posture across critical infrastructure sectors and government.
- developing and maintaining operational processes and playbooks for incident response across critical infrastructure and other key Australian sectors.
- developing public communications to improve the cyber security awareness of the Australian public and provide guidance of what individuals or impacted entities should do to respond to cyber incidents and how the Australian Government may support them.
- leading a National Cyber Exercise Program to exercise cyber crisis arrangements to ensure they are understood, integrated and rehearsed across government and industry.
- coordinating the delivery of the commitments and initiatives under the 2023-2030 Australian Cyber Security Strategy.

4.2. Response and relief

4.2.1. Tier of crisis coordination

The Australian Government will coordinate cyber incidents at its discretion. The Coordinator will assess and determine what tier of crisis coordination is required for each cyber incident, informed by advice from the NOCS. The Coordinator may also take advice from other Sector Lead or Enabling Agencies, such as the ASD's ACSC. This assessment is made by considering the principles-based crisis management guidance outlined in the AGCMF Handbook.

The Coordinator will regularly assess the cyber incident and, if required, change the tier of coordination. The tier may also be changed by another relevant decision maker as described in the AGCMF Handbook.

4.2.2. Australian Government coordination

The Coordinator and the NOCS will notify the office for the Minister for Cyber Security as well as key Australian Government stakeholders whenever it is coordinating the Australian Government response to a cyber incident. Refer to Section 2 for details of the Australian Government's coordination and response arrangements, in addition to the complementary arrangements by state and territory governments. Sector Lead Agencies and state and territory governments will often be responsible for relief to those impacted by a cyber incident. The Coordinator and the NOCS may have a prominent role in distributing communications and coordinating support services.

Cyber incidents often involve a sector or sectors across the Australian economy. Subject to agreement, the Australian Government Coordinating Agency may change from the NOCS where the nature of a cyber incident changes to predominantly affect a different Australian Government portfolio or where NEMA assumes the role.

4.2.3. Concluding Australian Government crisis coordination

The Coordinator as the Lead Coordinating Senior Official, or another relevant decision maker as described in the AGCMF Handbook, can make the decision to conclude the Australian Government's coordination of a cyber incident. This would include advising relevant stakeholders, standing down communication products and coordination mechanisms, and ensuring any continuing functions and responsibilities are clearly transferred to relevant officials and agencies, such as state and territory governments where applicable.

Indicators to stand down the Australian Government's coordination of a cyber incident may include, but are not limited to instances where:

- the impacted entity or entities have agreed that ongoing Australian Government coordination support is no longer required.
- other government agencies are best placed to carry any ongoing responsibilities or processes forward.
- the threats or demonstrable harm posed by the cyber incident are reduced or mitigated to an extent where Australian Government coordination is no longer required.
- there are no apparent steps that can be taken by the Coordinator or NOCS to support the incident.

4.2.4. Continuous improvement

The Coordinator and NOCS will regularly conduct post-incident evaluations of the Australian Government's response to cyber incidents to recognise any limitations, and enhance its coordination and consequence management arrangements for future incidents.

Within 12 months of any cyber incidents requiring Tier 3 coordination, the NOCS will conduct a whole of Australian Government evaluation with outcomes shared across the Australian Government and relevant stakeholders as soon as practical.

The scope of these evaluations may include:

- the arrangements supporting actions undertaken by and between Australian Government, state and territory governments and any impacted entities relating to consequences to be managed from the incident.
- specific consequence management issues related to cyber security, risk and the operation of cyber incident crisis response functions.
- how these arrangements supported decision making and information sharing.
- outcomes and actions underway to enhance incident coordination and consequence management arrangements.

NEMA is responsible for conducting evaluations for cyber incidents requiring Tier 4 coordination as the Australian Government Coordinating Agency.

4.3. Recovery

The Coordinator is responsible for the coordination of early recovery from a cyber incident.

The Crisis Recovery Coordination Plan (CRCP) provides the Australian Government a hazard agnostic, strategic and consistent whole-of-government approach to early recovery from a crisis. The CRCP recognises that states and territories maintain the primary responsibility for recovering from crises that occur in their jurisdiction, including cyber incidents.

Depending on the severity and nature of the incident, restoration of normal services and operations may vary across the several Australian Government and national arrangements highlighted under Section 2.2. The Coordinator and the NOCS will work with relevant government and industry entities to coordinate the restoration of services, systems and operations to minimise harms to the Australian public.

- As the lead technical authority, ASD's primary responsibility is the technical restoration and recovery of services and operations.

Where a cyber incident has tangible consequences such as disruptions to essential services, NEMA, in consultation with states and territories, will manage the recovery from those consequences in alignment with the defined Tiers set out in the AGCMF. Consideration should be given to the severity of impacts which may affect:

- Critical infrastructure assets, as defined through the *Security of Critical Infrastructure Act 2018*;
- The social or economic stability of Australia or its people;
- Significantly vulnerable communities;
- Commonwealth government and the government of a State or Territory;
- The defence or national security of Australia; and/or
- Other relevant factors considered by the Lead Minister to be of significant consequence, in consultation with other relevant ministers and stakeholders.

If a cyber incident requires longer-term considerations for recovery, the Coordinator may establish special purpose or temporary mechanisms to coordinate longer-term efforts across Australian, state and territory governments.

5. Reviewing AUSCYBERPLAN

The cyber security threat environment is continuously evolving alongside digital technologies, and so the national plan to coordinate the response to cyber incidents must evolve alongside it. Therefore the Coordinator, as the document owner, will review AUSCYBERPLAN annually or at their discretion, in consultation with relevant stakeholders or crisis response committees, following:

- post-incident reviews of AUSCYBERPLAN’s use in coordinating the response to cyber incidents
- exercises of AUSCYBERPLAN or exercises of specific arrangements identified within the AUSCYBERPLAN
- changes to the cyber security threat environment that would alter the Australian Government’s management of incidents
- relevant changes to the AGCMF, other coordination arrangements or the roles and responsibilities of Ministers, departments, agencies or entities listed in this document.

Minor amendments or updates impacting certain departments or agencies will be approved by the Coordinator in consultation with relevant departments or agencies.

6. Appendices

Appendix A	Acronyms and abbreviations
Appendix B	Reporting cyber security incidents to the Australian Government

Version	1.0
Document Owner	Cyber Security Preparedness and Response Branch, National Office of Cyber Security
Document Contact	NOCS.OperationalPlanning@homeaffairs.gov.au
Approver	National Cyber Security Coordinator
Approval Date	15 May 2025

Appendix A – Acronyms and abbreviations

ACSC	Australian Cyber Security Centre
AFP	Australian Federal Police
AGCCG	Australian Government Crisis Communication Guidelines
AGCMF	Australian Government Crisis Management Framework
AGCMF Handbook	Handbook to the Australian Government Crisis Management Framework
ANZPAA	Australian and New Zealand Policing Advisory Agency
ASD	Australian Signals Directorate
AUSCYBERPLAN	Australian Cyber Response Plan
AUSSECPLAN	Australian Government Domestic Security Crisis Plan
CCT	Crisis Coordination Team
CIMA	Cyber Incident Management Arrangements
COMDISPLAN	Australian Government Disaster Response Plan
Coordinator	National Cyber Security Coordinator
CRCP	Crisis Recovery Coordination Plan
CSRN*	Cyber Security Regulator Network
Home Affairs	Department of Home Affairs
IDETF	Inter-Departmental Emergency Taskforce
NCM	National Coordination Mechanism
NCTP	National Counter Terrorism Plan
NCSC	National Cyber Security Committee
NEMA	National Emergency Management Agency
NOCS	National Office of Cyber Security
NSC	National Security Committee of Cabinet
PM&C	Department of the Prime Minister and Cabinet
SOCI Act	*Security of Critical Infrastructure Act 2018*

**The CSRN comprises of the Australian Prudential Regulation Authority, the Office of the Australian Information Commissioner, the Australian Securities and Investments Commission, the Australian Communications and Media Authority, the Australian Competition and Consumer Commission, the Cyber and Infrastructure Security Centre within the Department of Home Affairs, the Reserve Bank of Australia, and the Treasury.*

Appendix B – Reporting cyber security incidents to the Australian Government

When cyber security incidents occur to private entities, those entities are encouraged to report those incidents as soon as possible to the Australian Government to seek support. This will allow the Australian Government to assess the incident, consider the potential scope and consequences from it and prepare or convene coordination mechanisms as required.

Organisations and individuals can get technical advice or help with an incident through the Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC).

For technical advice or to make a report:

- Contact the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371) for technical advice and assistance
- Visit the ReportCyber website to report a cybercrime or a cyber security incident.

Entities and individuals can report a cybercrime incident to the Australian Federal Police (AFP) or to state/territory police agencies through the ReportCyber website above.

For more information on regulatory reporting requirements, refer to the Single Reporting Portal.

Entities can contact the NOCS at nocs.response@homeaffairs.gov.au to seek advice on Australian Government coordination and consequence management support for their incident. Entities can also ask other government agencies to contact the NOCS on their behalf.

Engagement with the NOCS is voluntary. Its services complement existing structures and frameworks to enhance a private entity's incident response and consequence management activities. The NOCS is not a regulator and operates separately to an impacted entity's regulatory obligations.

The NOCS cannot support every entity that is experiencing a cyber security incident. The NOCS will only support an entity if their incident meets the threshold for being of national significance or interest.

If there is an immediate threat to life or risk of harm, always call 000.