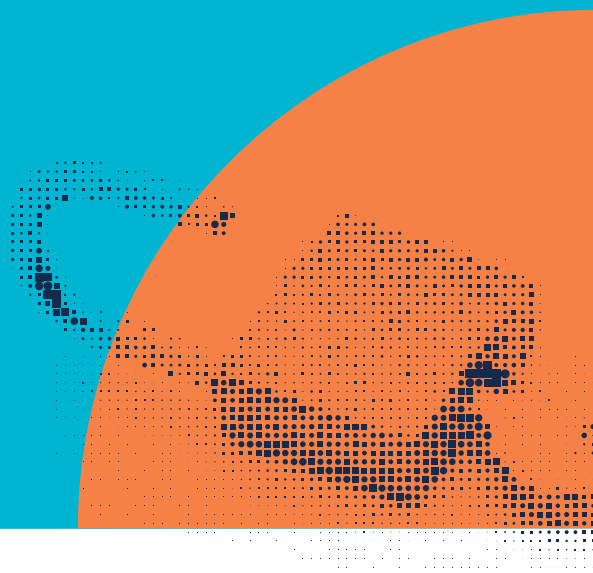
Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Cyber Incident **Management Arrangements** for Australian Governments



Context

The internet offers Australia significant economic, social and personal benefits. Australian governments, business and individuals are increasingly embracing the opportunities the internet offers.

Harnessing these opportunities also creates risks. The threat from malicious cyber activity against Australian interests is increasing in frequency, scale, sophistication and severity.

Cyber threats are often multi-dimensional and borderless in nature, and require an equally flexible response from those affected.

Managing cyber risks is a shared responsibility. Australian governments, business and individuals have a mutual responsibility to safeguard their use of the internet and digital systems.

Effective cyber security cannot be achieved in isolation. Partnerships between Australian governments, business and the community are key to advancing and protecting Australia's interests online.

Introduction

The aim of the Cyber Incident Management Arrangements (CIMA) for Australian governments is to reduce the scope, impact and severity of national cyber incidents on all Australians.

The CIMA provides Australian governments with guidance on how they will collaborate in response to, and reduce the harm associated with, national cyber incidents.

Scope

The CIMA outlines the inter-jurisdictional coordination arrangements, roles and responsibilities, and principles for Australian governments' cooperation in response to national cyber incidents.

The CIMA is not an operational incident management protocol. The detailed operational plans that underpin the CIMA will be jointly developed and maintained by Australian governments.

The CIMA supports, but does not replace, existing cyber incident management arrangements within each jurisdiction. Australian governments will continue to maintain their respective cyber incident management arrangements and will apply the CIMA to support national collaboration and coordination efforts.

The arrangements acknowledge that Australian business and community organisations may have existing cyber incident management arrangements, including arrangements for public communications and engagement. The CIMA may inform these existing arrangements by providing advice on anticipated Australian governments' response activities.

Relationship with crisis management arrangements

The CIMA is subordinate to, and does not change, existing national crisis management arrangements.

If a national cyber incident reaches a crisis level, the CIMA will support jurisdictions' respective crisis management arrangements, for example the Australian Government Crisis Management Framework (AGCMF).

Key Terms and Concepts

Cyber incident

A cyber incident is a single or series of unwanted or unexpected event(s) that impact the confidentiality, integrity or availability of a network or system or the information that it stores, processes or communicates.

National cyber incident

A national cyber incident is a cyber incident that:

- significantly impacts, or has the potential to significantly impact, multiple Australian jurisdictions, and/or
- requires a coordinated inter-jurisdictional response.

The incident could affect multiple jurisdictions simultaneously or could pose a threat to multiple jurisdictions after initially affecting a single jurisdiction.

Examples of potential national cyber incidents include:

- an organisation with links across multiple jurisdictions being compromised through a cyber incident
- malicious cyber activity affecting critical national infrastructure where the consequences have the **potential** to cause sustained disruption of essential services or threaten national security
- malicious cyber activity where the cause and potential extent of its geographic impact is uncertain, and
- a large-scale information system breach of sensitive data affecting persons or organisations in multiple jurisdictions.

A national cyber incident falls below the threshold required to activate national crisis arrangements, such as the Commonwealth's AGCMF. However, a national cyber incident may escalate to a crisis

in some circumstances – for example, if it results in sustained disruption to essential services, severe economic damage, a threat to national security or loss of life.

The precise escalation point from a national cyber incident to a crisis will be determined on a case-by-case basis, in accordance with existing crisis management arrangements.

Declaring a national cyber incident

The Australian Cyber Security Centre (ACSC) is the Australian Government's lead agency on national cyber security operational matters.

All Australian governments, business and the community are encouraged to report cyber incidents to the ACSC.

The ACSC assess all reported cyber incidents against an incident categorisation framework that considers the scope, impact and severity of an incident and its potential to harm Australia.

If a cyber incident significantly impacts, or has the potential to significantly impact, multiple Australian jurisdictions, and/or requires a coordinated inter-jurisdictional response, the ACSC may declare a national cyber incident in consultation with cyber security leads from affected Australian governments.

State and territory government cyber security leads may also request the ACSC declare a national cyber incident.

The declaration of a national cyber incident will activate the CIMA arrangements.

National Coordination Arrangements

Coordinating action during a national cyber incident

Upon declaring a national cyber incident, the National Cyber Security Committee (NCSC) will activate to support national collaboration and coordination of response efforts.

The NCSC is the peak cyber security coordination body for Australian governments. The NCSC provides strategic oversight and coordination of governments' cyber security policies and operational capabilities nationally.

The NCSC provides strategic coordination of national response efforts, and its members (or their representatives) are responsible for leading their jurisdiction's response to a national cyber incident.

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 escalates in impact and severity, the response may require escalation in accordance with existing national crisis management arrangements.

De-escalating a declared national cyber incident

When a cyber incident no longer significantly impacts, or has the potential to significantly impact, multiple Australian jurisdictions, and/or no longer requires a coordinated inter-jurisdictional response, the ACSC will issue advice to confirm the de-escalation of a national cyber incident. This process will occur in consultation with the NCSC.

Following the resolution of a national cyber incident, Australian governments and the ACSC may continue to provide the community with advice about the ongoing impacts of a cyber incident.

Roles and Responsibilities

The following section outlines the roles and responsibilities of Australian governments in responding to a national cyber incident.

State and Territory Governments

State and territory governments have primary responsibility for the protection of life, property and the environment within the bounds of their jurisdiction.

During a national cyber incident, NCSC members will lead their jurisdiction's input to the national coordination effort.

State and territory governments will:

- control their own jurisdictional response to an incident
- provide coordinated and consistent public information about the incident
- support inter-jurisdictional incident coordination via the NCSC
- provide the ACSC with information about cyber threats, vulnerabilities and mitigation strategies, for sharing nationally by the ACSC
- liaise with local government as necessary, and
- liaise with state and territory law enforcement agencies to assist with any criminal investigation into a national cyber incident.

Depending on the circumstances of a national cyber incident, it is possible that state and territory governments may adopt different response strategies that reflect the different impacts of the incident on their jurisdiction.

Where this occurs, the NCSC will coordinate national response efforts toward a shared goal of reducing the scope, impact and severity of national cyber incidents on the community.

Commonwealth Government

Department of Home Affairs
Home Affairs leads the coordinated development and implementation of national cyber security policy for the Australian Government.

Australian Cyber Security Centre
The ACSC is the Australian Government's lead agency on national cyber security operational matters.

The ACSC is part of the Australian Signals Directorate, and includes other Commonwealth agencies in a joint taskforce setting.

It brings together cyber security capabilities from across the Australian Government to improve the cyber resilience of the Australian community and support the economic and social prosperity of Australia in the digital age.

During a national cyber incident, the ACSC will:

- where practicable, provide technical resources and expertise to jurisdictions that require additional capacity or capability to respond to a national cyber incident
- collate, analyse and share information about cyber threats, impacts and mitigation strategies with Australian governments, business and the community

- lead public information on behalf of the Commonwealth Government, and develop and distribute key national messages to inform jurisdictions' own public messaging, and
- liaise with the Australian Intelligence Community, federal law enforcement and overseas jurisdictions to support national response efforts.

Joint Cyber Security Centres
The ACSC's Joint Cyber Security Centres (JCSCs), located in Sydney, Melbourne, Brisbane, Perth and Adelaide, bring together business and the research community along with state, territory and Australian Government agencies in an open and cooperative environment. They provide a venue for local coordination activity, and will support consequence assessment and liaison with various organisations as necessary.

The JCSCs facilitate rapid information sharing between governments and business, and enable organisations to develop joint solutions to complex and shared cyber security problems.

Business and the community

Although it does not apply to business and the community, private entities may use the CIMA to understand Australian governments' response activities during a national cyber incident.

During a national cyber incident, business and the community remain responsible for protecting their assets, including information stored on their systems, from malicious cyber activity.

Business and the community should consider public information provided by Australian governments during a national cyber incident to inform their understanding of:

- the circumstances of an incident
- potential risk mitigation and remediation strategies, and
- the potential for community impacts and warning advice.

Various resources currently exist to support business and the community in protecting their systems from malicious cyber activity. Important information can be found at **https://cyber.gov.au**.

Strategic Principles for using the CIMA

The CIMA's principles provide a basis for Australian governments' cooperation on responses to national cyber incidents.

Protecting Australia's interests

In responding to a national cyber incident, Australian governments will prioritise preserving Australia's national interests, including public safety, the delivery of essential services and maintaining national security.

Shared responsibility

Australian governments have a shared responsibility to build resilience, transparency and trust in our online systems and, ultimately, to protect Australia from the effects of national cyber incidents.

This responsibility also extends to business and the community, including small, medium and large businesses, which are responsible for maintaining their own cyber security.

Collaboration for harm minimisation

A collaborative and mutually supportive approach to national cyber incident management including, where practicable, sharing expertise and resources, will maximise the effectiveness of national response efforts and assist in reducing the scope, impact and severity of national cyber incidents.

Consistent public information

A coordinated approach to public information in a national cyber incident will support consistent messages that improve businesses' and the community's understanding of the incident and recommended actions.

Continuous improvement

Australian governments, business and the community are encouraged to share lessons arising from national cyber incidents to continually improve response arrangements. Arrangements must keep pace with the changing cyber landscape and threat picture.

Accountable & transparent

Decision-making and actions in response to a national cyber incident should be transparent and accountable, subject to national security, privacy and other legal considerations.

Benefits of using the CIMA

Through enhanced coordination, the CIMA supports more effective and timely responses to national cyber incidents by providing a structured framework for cooperation between Australian governments.

The benefits of strong strategic inter-jurisdictional coordination include:

- improved situational awareness across jurisdictions, which increases the effectiveness and timeliness of response activities
- potential to prevent a national cyber incident from escalating to a national crisis
- more efficient use of jurisdictional response resources, and
- consistent public information from Australian governments to business and the community, to promote confidence and contain the potential spread of a cyber incident.

Exercising the Arrangements

The arrangements will be exercised and strengthened as part of the ACSC National Exercise Program in partnership with Australian governments, business and international cyber security partners.

Outcomes from the exercises will inform continuous improvement of the arrangements.

Governance and Review

The arrangements are owned and maintained by the NCSC.

The arrangements will be reviewed every three years by the NCSC in consultation with relevant stakeholders.

More frequent reviews may be undertaken if required, including following the activation or exercising of the arrangements.

Appendix.

A National Cyber Incident Management Arrangements (CIMA) for Australian Governments.