Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Cyber Incident Management Arrangements

for Australian Governments

1. Context

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

1.2 Harnessing these opportunities also creates risks. The threat from malicious cyber activity against Australian interests is increasing in frequency and impact.

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

1.4 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.

1.5 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.

1.6 Australians expect governments will play a leading role in preparing for and responding to cyber security incidents, including managing consequences to reduce the potential for harm to the community.

2. Introduction

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

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

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

3. Benefits of using the CIMA

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

3.2 The benefits of strong inter-jurisdictional coordination include:

- improved situational awareness across jurisdictions, which increases the effectiveness and timeliness of response activities
- potential to prevent a national cyber security incident from escalating to a national crisis, including by preventing the potential spread of a cyber security incident
- more efficient use of jurisdictional response resources, and
- consistent public information from Australian governments to business and the community, to support cyber security preparedness and response activities, including for consequence management.

3.3 The CIMA works within the context of the Australian Government Crisis Management Framework (AGCMF) to ensure Australian governments effectively manage the second and subsequent order consequences of cyber security incidents.

4. Scope

4.1 The CIMA outlines the inter-jurisdictional coordination arrangements, roles and responsibilities, and principles for Australian governments' cooperation in preparation for and in response to national cyber security incidents. This includes activities to prepare for and reduce the harm and consequences of cyber security incidents.

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

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

4.4 The arrangements acknowledge that Australian business and community organisations may have existing cyber security incident management arrangements, including arrangements for public communications and engagement. The CIMA encourages coordinated and consistent public messaging between Australian governments and private industry organisations during cyber security incidents.

Relationship with crisis management arrangements

4.5 The Australian Government Crisis Management Framework (AGCMF) outlines the Australian Government's approach to preparing for, responding to and recovering from crises. The AGCMF recognises that the 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.

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

4.7 If a national cyber security incident occurs, the CIMA will support jurisdictions' respective crisis management arrangements by activating the Australian Government crisis arrangements under the AGCMF should this be required. Arrangements could include convening the Australian Government Crisis and Recovery Committee (AGCRC) to bring together Australian Government agencies and/or convening the National Coordination Mechanism (NCM) to bring together jurisdictions, Australian Government agencies and/or industry.

4.8 If a national cyber security incident reaches crisis level, the CIMA will support jurisdictions' respective crisis management arrangements by activating the Australian Government crisis arrangements under the AGCFM through the AGCRC or NCM. In addition, national consequence management responses may be supported by the Australian Government's National Situation Room (NSR) and led by the formation of an Australian Government Crisis Coordination Team (CCT). The NCM, NSR and CCT are administered by NEMA. CCTs may be collaborative teams formed by members of NEMA, and relevant agencies such as the Department of Home Affairs, the Australian Signals Directorate's Australian Cyber Security Centre and other Australian Government agencies to manage the consequences of a particular crisis event.

5. Key Terms and Concepts

Cyber security incident

5.1 A cyber security 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.

5.2 Cyber security incidents can be caused by cyber criminals, nation state actors, political 'hacktivists' and online vandals. They can significantly disrupt the delivery of critical infrastructure and essential services, as well as causing:

- damage to personal identity and reputation
- financial loss, business disruption and reputational damage
- impact on emotional and psychological wellbeing.

5.3 The outcomes of cyber security incidents can have significant and long-lasting consequences for government, industry and the community.

Data breach

5.4 A data breach occurs when data is inadvertently shared with or maliciously accessed by an unauthorised party. A data breach may require a cyber security incident response if there is ongoing impact to the confidentiality, integrity or availability of a network or system.

5.5 A consequence management response may be required to reduce the harms that result from a data breach.

Consequence management

5.6 Consequence management relates to the second and subsequent order effects from cyber security incidents. It requires government and industry to work together to identify and mitigate the secondary harms that may result from a cyber security incident. In the most severe instances, this could include 'real world' impacts requiring the activation of emergency management arrangements, such as the NCM and, in cyber crises, the NSR and CCT.

5.7 Consequences that could arise from a cyber security incident could include:

- disruptions to government and the provision of government services, including those delivered both in-person (e.g. front-line health care) or online (e.g. government payment systems)
- disruptions to critical infrastructure, critical goods and the provision of essential services upon which the community relies, including those owned or operated by governments (e.g. energy, water and sewerage) or by the private sector (e.g. airports, medical supplies, freight networks)
- large scale data breaches of government or personal identity data and subsequent criminal activity, which might require the re-issuing of credentials and increased levels of security applied to compromised identities

National cyber security incident

5.8 A national cyber security incident is a cyber security incident that:

- significantly impacts, or has the potential

to significantly impact, multiple Australian jurisdictions either simultaneously or through spread to other jurisdictions, and/or

- requires a coordinated inter-jurisdictional cyber security incident response and may include the separate activation of consequence management mechanisms.

5.9 Examples of potential national cyber security incidents include:

- an organisation with links across multiple jurisdictions being compromised through a cyber security incident
- malicious cyber activity affecting critical national infrastructure where the consequences have the potential to cause sustained disruption to the supply of essential goods and services to the Australian community or threaten national security
- malicious cyber activity where the cause and potential extent of its geographic impact is uncertain.

Declaring a national cyber security incident

5.10 The Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) is the Australian Government's lead agency on national cyber security operational matters, including technical cyber security incident response and advice.

5.11 The National Cyber Security Coordinator will lead on consequence management activities for the Commonwealth government in collaboration with NEMA or Australian Governments.

5.12 ASD's ACSC and state and territory governments assess all reported cyber security incidents against incident categorisation frameworks that consider the scope, impact and severity of an incident and its potential to harm Australia or relevant jurisdictions.

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

5.14 State and territory government cyber security leads may also request that ASD's ACSC convene the National Cyber Security Committee (NCSC) to discuss and then potentially declare a national cyber security incident.

5.15 If a national cyber security incident is declared, the National Cyber Security Coordinator in collaboration with NEMA may activate the consequence management mechanisms, such as the NCM, to coordinate jurisdiction and/or Australian Government response to the crisis.

From national cyber security incident to national cyber crisis

5.16 A national cyber security incident will not automatically activate national crisis arrangements. A national cyber security incident may escalate to a crisis in some circumstances – for example, if it results in sustained disruption to the supply of essential goods and services, severe economic damage, a threat to national security, loss of life, formal ministerial consideration of the event or where there is community expectation of national leadership.

5.17 The decision to escalate a national cyber security incident to a national cyber crisis will be determined on a case-by-case basis by the National Cyber Security Committee (NCSC, in collaboration with the National Cyber Security Coordinator and NEMA, to ensure that consequence management is activated as appropriate.

5.18 National, states or territory crisis management or consequence management arrangements may be activated independently when conditions necessitate, irrespective of the type of cyber security incident

De-escalating a declared national cyber security incident or crisis

5.19 When a national cyber security 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, ASD's ACSC will issue advice to confirm the de-escalation of a national cyber security incident. This process will occur in consultation with the NCSC.

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

Protecting Australia's interests

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

Shared responsibility

5.22 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 cyber security incidents.

5.23 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

5.24 A collaborative and mutually supportive approach to national cyber security 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 security incidents.

Consistent public information

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

Continuous improvement

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

Accountable & transparent

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

6. Roles and Responsibilities

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

National Cyber Security Committee

6.2 The National Cyber Security Committee (NCSC) is the mechanism for inter-jurisdictional coordination for cyber security incident response. The NCSC members include the Head of the Australian Signals Directorate's Australian Cyber Security Centre, the cyber security state and territory lead from each jurisdiction, and supporting representatives from the Department of Home Affairs, the National Emergency Management Agency, the Australian Federal Police and the Department of Prime Minister and Cabinet. The National Cyber Security Coordinator may be invited as required. The NCSC is co-chaired by the Head of the Australian Cyber Security Centre and a cyber security lead from a state or territory.

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

6.4 The NCSC's role in responding to a national cyber security incident includes:

- facilitating the exchange of threat intelligence and solutions to enhance jurisdictions' situational awareness and response activities
- assisting consequence management activities, including the identification of harms and harm assessment in collaboration with the National Cyber Security Coordinator
- overseeing the development of nationally consistent public information
- determining the National Cyber Security Arrangements level
- 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.

6.5 If a national cyber security incident escalates in impact and severity, the response may require escalation in accordance with existing national crisis management arrangements, in collaboration with the National Cyber Security Coordinator and NEMA, to ensure that consequence management is activated as appropriate.

State and Territory Governments

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

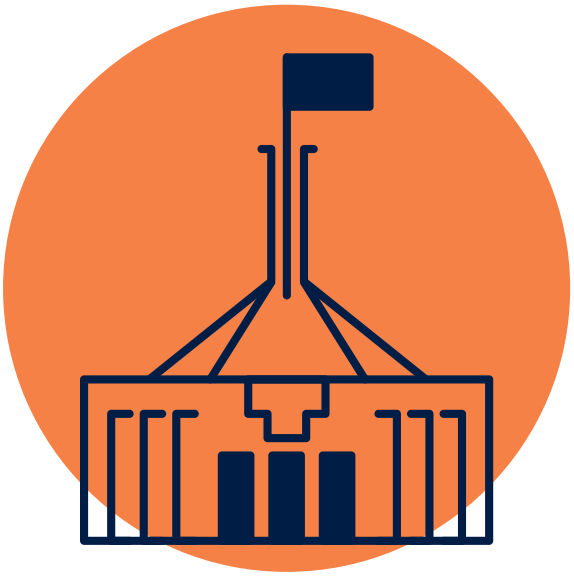
6.7 NCSC members will lead their jurisdiction's input to the national cyber security incident coordination effort.

6.8 State and territory governments will:

- control their own jurisdictional cyber security incident response and consequence management activities to an incident
- provide coordinated and consistent public information about the incident
- support inter-jurisdictional cyber security incident coordination via the NCSC
- support inter-jurisdictional consequence management activities, including via the National Cyber Security Coordinator and NCM; and in cyber crises through other Australian Government national consequence management activities such as the NSR and CCT.
- provide ASD's ACSC with information about cyber threats, vulnerabilities and mitigation strategies, for sharing nationally by ASD's 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 security incident.

6.9 Depending on the circumstances of a national cyber security 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.

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



Commonwealth Government Australian Signals Directorate's Australian Cyber Security Centre

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

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

6.13 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.

6.14 During a national cyber security incident, ASD's ACSC will:

- where practicable, provide technical resources and expertise to jurisdictions that require additional capacity or capability to respond to a national cyber security incident
- collate, analyse and share information about cyber threats, impacts and mitigation strategies with Australian governments, business and the community
- lead public cyber security incident technical information on behalf of the Commonwealth Government in consultation with the National Cyber Security Coordinator, 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.

National Cyber Security Coordinator

6.15 The National Cyber Security Coordinator will lead, across the Australian Government, the coordination and triaging of action in response to a major cyber security incident. They will also ensure the Minister for Cyber Security has access to all the information required to effectively oversee the whole-of-government response to a major cyber security incident. The Coordinator is supported by the National Office of Cyber Security within the Department of Home Affairs and draws upon the resources of the Department as required to support their activities.

6.16 During a nationally significant cyber security incident, the National Cyber Security Coordinator will coordinate the activities of the Australian Government and work through the NCSC to collaborate on cyber security issues. The incident response functions of State and Territory Governments, and the Australian Signals Directorate or the Australian Federal Police, will maintain

operational independence.

Department of Home Affairs

6.17 The Department of Home Affairs leads the development and implementation of cyber security policy for the Australian Government. Through the Cyber and Infrastructure Security Centre, the Department is the cyber security regulator for critical infrastructure sectors and administers the cyber security incident response powers as contained in the Security of Critical Infrastructure Act 2018 (Cth).

6.18 During a cyber security incident, the Department coordinates consequence management activities for nationally significant cyber security incidents. The Department will work alongside Commonwealth agencies which lead technical incident responses, law enforcement operations, regulatory activities, and emergency management.

6.19 The Department will:

- support the Coordinator to perform their coordination function;
- engage with the National Emergency Management Agency (NEMA) on the potential activation of the National Coordination Mechanism (NCM); and in the event of a national cyber crisis, engage with NEMA on the engagement of the NSR and activation of the CCT;
- convene working groups as required to allow Australian government departments or agencies to efficiently undertake specific lines of effort within consequence management;
- lead Commonwealth consequence management activities undertaken to support a single state or territory to engage with relevant Commonwealth departments or agencies; or
- support impacted entities to engage with Commonwealth, state, or territory departments and agencies on cyber security incidents

National Emergency Management Agency

6.20 NEMA is an executive agency in the Home Affairs portfolio. Through the AGCRC and NCM, NEMA supports consequence management under the AGCMF which may include supporting the national consequences of cyber security incidents and crises.

6.21 As requested by the National Cyber Security Coordinator and/or Department of Home Affairs, NEMA will facilitate and co-chair the AGCRC and/or NCM to assist government to manage the consequences of cyber security incidents and crises.

6.22 NEMA will lead the whole-of-government coordination of a response to a cyber security incident that has nationally significant consequences on services, supply chains and systems that directly impact or have potential to impact Australian community, society and industry.

6.23 The Australian Government NSR (managed by NEMA) will provide notifications and maintain situational awareness of cyber security incidents and crises that are of national significance and consequence.

6.24 Australian Government CCTs may be stood up within the NSR to coordinate national crisis consequence management, in collaboration with the Department of Home Affairs and with support from other relevant government agencies.

The Department of Prime Minister and Cabinet

6.25 The Department of Prime Minister and Cabinet (PM&C) provides advice to the Prime Minister on cyber security policy, implementation and incident response. PM&C is also responsible for setting, and oversight of, Commonwealth crisis management policy, in accordance with the AGCMF.

Law Enforcement

6.26 Commonwealth, State and Territory law enforcement agencies are responsible for the investigation of cybercrime. When a national cyber security incident occurs it is important to notify law enforcement as early as practicable so the appropriate law enforcement response can be determined and relevant advice provided to the affected entities. Law enforcement agencies will work with both government and private sector incident responders to preserve and gather evidence to progress the criminal investigation. The identification, disruption and/or prosecution of the offender/s behind an incident is an important component of the response and may deter future offending.

6.27 Under national law enforcement coordination arrangements for cybercrime, the Australian Federal Police (AFP) is responsible for investigating cybercrimes against a Commonwealth Government entity, critical infrastructure and information systems of national significance or where the cybercrime offences impact the whole of the Australian economy. Most cybercrimes under the remit of the CIMA will involve the AFP. However, where the victim is a State or Territory government entity the law enforcement agency in that State or Territory has responsibility for any criminal investigation.

6.28 The AFP will coordinate with State and Territory law enforcement agencies regarding the criminal investigation/s into national cyber security incidents, including determining which agency will have responsibility for the investigation. There are existing coordination mechanisms that have been established for law enforcement, including the AFP-led Joint Policing Cybercrime Coordination Centre (JPC3). The JPC3 may, where appropriate, coordinate an Australian law

enforcement response that minimises and prevents the threat/harm from the misuse of sensitive and personally identifiable information (PII) resulting from an incident. This includes identifying, disrupting, charging and prosecuting any person seeking to exploit sensitive PII derived from major national data breaches impacting Australians.

Business and the community

6.29 Business and the community may use the CIMA to understand Australian governments' response activities during a national cyber security incident.

6.30 All businesses, including critical infrastructure and small and medium enterprises, and the community remain responsible at all times for protecting their assets, including information stored on their systems, from malicious cyber activity.

6.31 Business and the community should consider public information provided by Australian governments during a national cyber security 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.

6.32 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.

6.33 Commonwealth facilities may be made available to securely exchange sensitive cyber security incident response information with Australian Governments, business and industry.

7. Exercising the Arrangements

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

7.2 The NCSC will review exercise outcomes to inform continuous improvement of the arrangements.

7.3 The National Cyber Security Coordinator will coordinate a national cyber security exercise program across the Australian Government. These exercises will be delivered by Commonwealth departments and agencies in partnership with states, territories, and industry. This could include cyber security exercises focused on technical incident responses, consequence management activities, all hazards emergency management activities, and sector-specific issues.

8. Governance and Review

8.1 The arrangements are owned and maintained by the NCSC.

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

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

9. Appendix

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