Higher Education and Research Sector Playbook

The Higher Education and Research Sector Playbook (the playbook) is a high level guide for how the National Office of Cyber Security (NOCS) will coordinate the national response and consequence management activities for a cyber incident impacting an entity in the sector. The playbook outlines how the NOCS will support the impacted entity, government and broader industry response. It highlights how the NOCS will work with the impacted entity and key government and industry stakeholders with a direct interest in the incident, its impacts and the response. The playbook does not provide a prescriptive response to be applied to all incidents impacting the sector. Each response will differ depending on the nature of the incident, the impacted entity and the need for coordinated consequence management activities. The playbook is a living document and will be routinely reviewed and updated following incidents, exercises and feedback. Further information about the NOCS and its services can be found at www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-coordinator.

INITIAL RESPONSE

Notification of an incident

Impacted entities should report cyber incidents to ASD before notifying the NOCS. www.cyber.gov.au/report is the place to report a cyber incident to ASD.

The NOCS could then be notified that an incident is impacting a higher education and research entity via different channels including direct notification from the impacted entity, its third party service providers, or other Australian Government or state and territory government agencies.

Directly emailing NOCS.Response@homeaffairs.gov.au is the most effective way to ensure the NOCS is aware of an incident and to seek advice on whole-of-government coordination and consequence management support.

Impacted entities should also notify relevant regulators as required. The NOCS is not a regulator and operates separate to an impacted entity's regulatory obligations.

Part 4 of the *Cyber Security Act 2024* establishes a limited use obligation that restricts how the National Cyber Security Coordinator and the NOCS can record, use or disclose information that a higher education and research entity or another entity acting on their behalf voluntarily provide under Part 4 in specified circumstances. Additional information on the limited use obligation can be found through the NOCS webpage above.*Initial engagement with impacted entity*

The NOCS will engage with ASD in the first instance to understand the incident and inform the timing and nature of the NOCS' initial engagement with the impacted entity.

Engagement with the NOCS is voluntary. Its services complement existing structures/frameworks to enhance an impacted entity's incident response, coordinate government and industry responses to incidents, and manage the consequences of incidents.

Once notified of an incident, the NOCS will engage the impacted entity to:

- gain an initial view of the nature of the incident, systems/information affected, and potential or actual impact
- determine who is already assisting with the response (e.g. third-party incident response, ASD and/or AFP) and who has been advised (e.g. regulators and/or relevant state and territory governments)
- provide an overview of the NOCS' role and outline next steps, including establishing whether the NOCS can add value by coordinating the response, and
- consider whether the impacted entity requires additional support from other government entities.

The NOCS will engage other government agencies, including key policy departments, regulators, state and territory agencies, and key forums and committees to understand interests and inform understanding of potential consequences.

To encourage the transparent and timely sharing of information between the NOCS and the impacted entity, the NOCS operates under Australian Government security classifications and will adopt the Traffic Light Protocol (www.cyber.gov.au/tlp) when dealing with information provided by an impacted entity.

Assess consequences

Informed by initial assessment and discussions, the NOCS will assess potential consequences, considering:

- safety of individuals
- potential impacts to the Australian Government and state and territory governments, such as the exposure of government information
- potential impacts to other entities, including to critical infrastructure, such as the exposure of sensitive research, operational or corporate data
- sectoral impacts, depending on nature, jurisdiction and/or specialisation of the higher education and research entity
- customer trust (institutional/service provision) of services
- any public statements or market announcements planned or released
- exposure of:
  - personal information
  - ID credentials
  - information relating to vulnerable persons
  - national security or law enforcement information
  - sensitive corporate or commercial information, including intellectual property
- any other potential or actual consequence identified, based on the specific incident.

Categorise incident

The Australian Government Crisis Management Framework 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 an incident will guide the determination of appropriate coordination efforts to be provided by the NOCS and other responding agencies and departments.

The NOCS will categorise the incident on the following scale, as determined by national thresholds:

- 'nationally catastrophic incident', which might require leadership by the Prime Minister
- 'nationally significant incident', which might require leadership by the Minister for Cyber Security or the National Cyber Security Coordinator (Coordinator)
- 'significant incident', which might require leadership by the NOCS, or
- 'incident', which might require the NOCS to support another government agency leading a response.

Categorisation considerations include:

- What is the nature of the incident?
- Is there potential for harm?
- Does it affect a large portion of the population?
- Does it involve multiple jurisdictions?
- Is there high media/political interest?
- Is the NOCS able to add value through coordinating the response?

Engaging the Coordinator and the Minister

The NOCS will advise the Coordinator on the nature of the incident, the response required and any requirement to brief the Minister for Cyber Security.

COORDINATED RESPONSE

Initial briefings for shared situational awareness

The NOCS will initially meet with the impacted entity or its designated representative to understand the nature and extent of the incident.

In consultation with the impacted entity, the NOCS may also convene an initial briefing with the impacted entity and relevant Australian Government and state and territory government agencies. The briefing will provide an overview of the incident, consider its potential impacts and discuss the requirement for coordinated consequence management activity. This may include representatives from state and territory cyber response agencies who are best-equipped to provide advice on potential impacts within their jurisdictions.

Where the impacted entity has government clients, a government agency may be involved as both a stakeholder in the coordinated response and also as an impacted entity. Consideration will be given to the management of these differing interests to separate commercial and legal

considerations from broader consequence management activities.

Public communications

The NOCS will coordinate a consistent public communications approach across government and consult with the impacted entity to support alignment of public messaging throughout the response. Ownership and endorsement of business-specific messaging will remain with the impacted entity.

Working groups for coordination and consequence management

Following this, the NOCS may establish working groups based on the specific nature of the incident and what data/systems/impacts are assessed as requiring a coordinated response. The NOCS will leverage existing forums and committees, where appropriate.

The impacted entity may provide situational updates to working groups. The impacted entity may not be required for all working group meetings or the entirety of a meeting if discussion focuses on specific government processes.

For the higher education and research sector, specific coordinated response working groups the NOCS may convene include:

- **Chief Information Security Officer Working Group (CISOWG)** – A CISOWG could be convened by ASD's ACSC with the NOCS' support for secretariat purposes. The CISOWG could include representatives from the impacted entity; their third party service provider; relevant representatives from the Australian Government and state and territory governments; and relevant industry representatives. A CISOWG could discuss technical issues to support the impacted entity to respond to the incident and mitigate potential technical impacts to government and industry stakeholders from the incident.
- **Higher Education and Research Sector – Government Working Group (HERS–GWG) –** The HERS-GWG could include relevant representatives from the impacted entity; their third party service provider; the Australian Government and state and territory governments. The primary function of the HERS–GWG would be to consider the impact of the incident on the sector, and the coordinated activities required to support the entity to respond to the incident and its impact on the delivery of services in the sector.
- **Higher Education and Research Sector – Industry Working Group (HERS–IWG) -** The HERS–IWG could include relevant representatives from; the impacted entity; peak bodies; industry entities and organisations, (e.g. AHECS); third parties (e.g. service providers that need to remain up-to-date on the incident and may themselves be secondarily impacted entities), and the Australian Government and state and territory governments. Attendance is subject to consent from the primary impacted entity to ensure messaging is targeted and considers the 'need to know' principle of information sharing.
    - The ACCC, OAIC, and relevant state and territory information and privacy bodies may be invited depending on the nature of the incident and the impacted entity involved.
- **Communications Working Group (CWG) –** The primary function of the CWG is to provide media/communications representatives from the relevant government departments and agencies with a forum to discuss and coordinate public communications during an incident, including the alignment of messaging and timing of notifications.
    - The CWG is chaired by NOCS Crisis Media. The impacted entity will be invited to ensure alignment of public communications from government and the impacted entity. However, the impacted entity may be excused from discussions focused on government communications issues.
- **Data Review Working Group (DRWG) –** The DRWG brings together technical experts assisting the impacted entity and government specialists to better support the entity in its data review process. DRWG efforts may include addressing complex data analysis issues, informing the data discovery process and refining search terms to enable effective data assessment and remediation efforts.
- **Identity Services and Security Working Group (IDSSWG) –** The IDSSWG will primarily be required for data breaches impacting personally identifiable information. The IDSSWG enables credential issuing bodies, service providers, regulators and other relevant stakeholders to discuss and align their response to these incidents, improving the timeliness, effectiveness and efficiency of remediation activity.

- The IDSSWG is co-chaired by Services Australia and AGD, with the NOCS providing secretariat and briefing support.
- The IDSSWG will include Services Australia, AGD, ATO, DFAT, AFP and representatives from credential issuing bodies of relevant state and territory governments. OAIC may also be invited to support general policy guidance.

- **Sensitive Issues Working Group (SIWG) –** The SIWG may include representatives from agencies concerned that particularly sensitive information may have been exposed, for example, information relating to vulnerable persons, sensitive health information, national security or law enforcement information etc.

Where possible, working groups are streamlined to avoid duplication, reduce overhead and enable proactive response.

National Coordination Mechanism

Alongside ongoing assessment of an incident, an NCM may be held. For cyber incidents, the Coordinator co-chairs the NCM with Deputy Coordinator-General, Emergency Management and Response, NEMA.

An NCM could be held at the start of an incident to provide shared situational awareness of an incident, understand the potential impacts of an incident, identify lines of effort required to manage the consequences of an incident, and establish working groups or task existing working groups.

During an NCM:

- the impacted entity provides an update to participants to support situational awareness
- discussion occurs on problem definition, impacts and consequence management
- lines of effort are agreed to mitigate impacts and consequences, and
- attendees can ask questions or comment on issues of concern or relevance.

These meetings will be maintained at a cadence appropriate to the level of coordination and communication required, and in consultation with the impacted entity and relevant stakeholders.

Additional information on the NCM can be found here.

POST COORDINATED RESPONSE

Ceasing the coordinated response

The NOCS will cease coordination and consequence management activities when a coordinated approach is no longer required, in consultation with the impacted entity.

If required, the NOCS will assist with facilitating bilateral engagement between the impacted entity and any key stakeholders that remain involved in the post-coordinated response. This will support continuity and the resolution of any emerging issues which might benefit from whole-of-government coordination.

Lessons learned

The finalisation of coordination and consequence management activities may include a post-incident review, conducted in consultation with the impacted entity, relevant industry stakeholders, and Australian Government and state and territory government agencies.

This will be supported, where appropriate, by the development of a public communications response on key ‘lessons learned’ to uplift Australia’s cyber resilience and security, in consultation with the impacted entity.

ACRONYMS

ACCC	*Australian Competition and Consumer Commission*
ACSC	*Australian Cyber Security Centre*
AFP	*Australian Federal Police*
AGD	*Attorney-General's Department*
AHECS	*Australian Higher Education Cybersecurity Service*
ASD	*Australian Signals Directorate*
ATO	*Australian Taxation Office*
CISOWG	*Chief Information Security Officer Working Group*
CWG	*Communications Working Group*
DFAT	*Department of Foreign Affairs and Trade*
DRWG	*Data Review Working Group*
HEIRSG	Higher Education, Innovation and Research Sector Group
HERS-GWG	*Higher Education and Research Sector – Government Working Group*
HERS-IWG	*Higher Education and Research Sector – Industry Working Group*
IDSSWG	*Identity Services and Security Working Group*
NCM	*National Coordination Mechanism*
NEMA	*National Emergency Management Agency*
NOCS	*National Office of Cyber Security*
OAIC	*Office of the Australian Information Commissioner*
SIWG	*Sensitive Issues Working Group*

Version *1.0*
Date *09 July 2025*