FACTSHEET: Limited Use for the National Cyber Security Coordinator

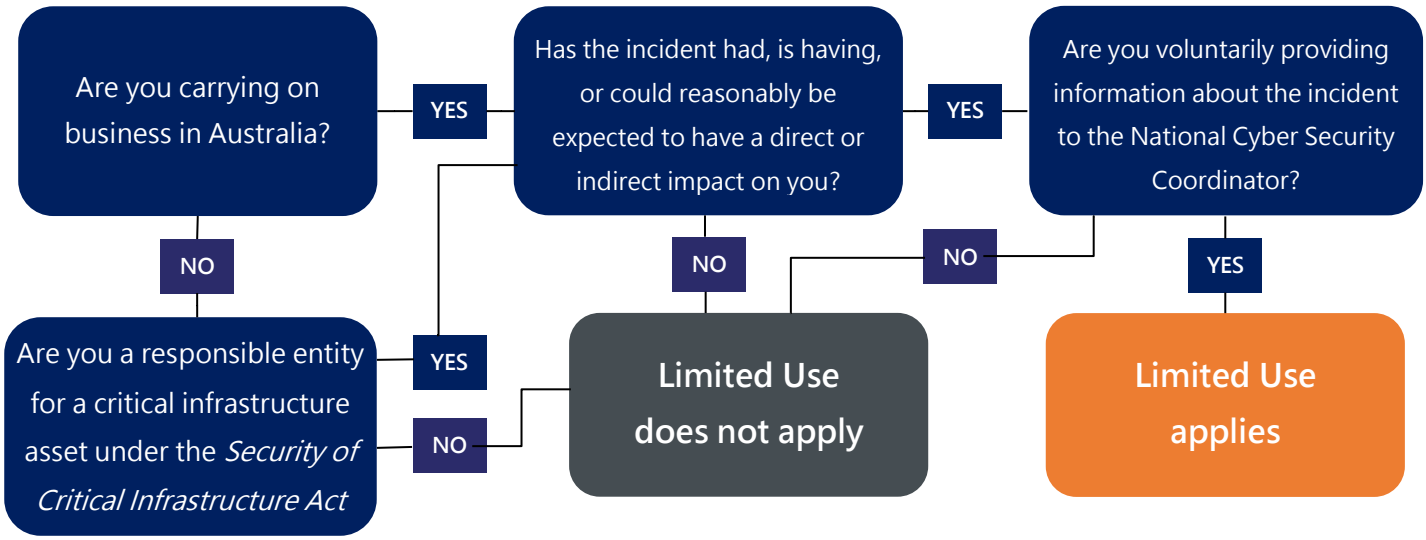
What is the limited use obligation?

Part 4 of the *Cyber Security Act 2024* establishes a limited use obligation that restricts how the National Cyber Security Coordinator (the Coordinator) and the National Office of Cyber Security can record, use or disclose information that you or another entity acting on your behalf voluntarily provide under Part 4 in specified circumstances.

The role of the Coordinator is to lead whole-of-government coordination in response to significant cyber security incidents. The objective of the limited use obligation is to provide you the confidence to engage early and share information freely, without fear that the Coordinator will provide your information to regulators or law enforcement for use in regulatory or law enforcement proceedings. Please note that information provided to the Coordinator can be recorded, used or disclosed for the purposes of investigating or enforcing whether you have contravened Part 4 of the *Cyber Security Act 2024* or a law that imposes a penalty or sanction for a criminal offence.

Will limited use apply to my information?

The following questions will assist you in understanding whether limited use applies to the information you are providing the Coordinator:



The information contained in this document is general in nature and does not constitute legal advice. Readers are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.

If the answer is yes to all of the above questions, then the limited use obligation applies to the information you or another entity acting on your behalf, voluntarily provide to the Coordinator. Please also note that your information is protected even if it is not a cyber security incident, or if it is not a significant cyber security incident – more information below.

What is a significant cyber security incident?

A cyber security incident is significant if there is a material risk that the incident has seriously prejudiced, is seriously prejudicing, or could reasonably be expected to prejudice:

- the social or economic stability of Australia or its people, or
- the defence of Australia, or
- national security.

A cyber security incident is also significant if the incident is, or could reasonably be expected to be, of serious concern to the Australian people.

The terms ‘seriously prejudice’ and ‘serious concern’ have their ordinary meanings and are an important criteria to establish whether an incident is of sufficient seriousness. In the context of limited use, ‘seriously prejudiced' and ‘serious concern’ are designed to ensure that the National Cyber Security Coordinator has the primary role in leading across the whole-of-government the coordination and triaging in response to significant cyber security incidents that could reasonably be considered capable of causing significant damage or harm to Australian interests.

An incident may meet this criterion even if it does not have an impact on all jurisdictions, but rather the impact to Australia’s national interests, recognising that an impact on, for example, a particular part of the economy, may also be nationally significant.

What can the Government do with limited use information?

For significant cyber security incidents, the Coordinator may only record, use or disclose information to assist the impacted entities, and other entities acting on behalf of the impacted entity to respond to, mitigate or resolve the cyber security incident, or for **permitted cyber security purposes** where the limited use obligation applies. This means that the Coordinator can record, use or disclose information for:

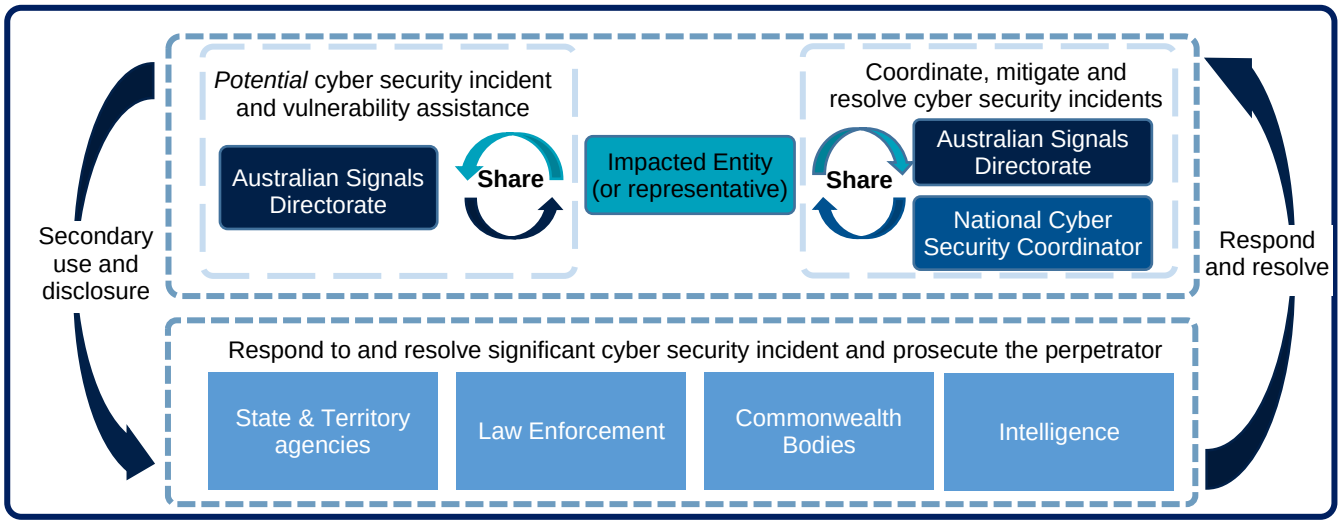
- the performance of the functions of a Commonwealth body (to the extent that it is not a Commonwealth enforcement body) relating to responding to, mitigating or resolving the cyber security incident
- the performance of the functions of a state body relating to responding to, mitigating or resolving the cyber security incident
- the performance of the functions of the Coordinator under Part 4 of the *Cyber Security Act 2024* relating to the cyber security incident
- informing and advising the Minister for Cyber Security, and other Ministers of the Commonwealth, about the cyber security incident
- preventing or mitigating material risks that the cyber security incident has seriously prejudiced, is seriously prejudicing, or could reasonably be expected to prejudice the social or economic stability of Australia or its people, the defence of Australia, or national security
- preventing or mitigating material risks to a critical infrastructure asset
- the performance of the functions of an intelligence agency, and

- the performance of functions of a Commonwealth enforcement body (except for the purposes of investigating or enforcing, or assisting in the investigation or enforcement of, any contravention by the impacted entity of a Commonwealth, State or Territory law, other than a contravention of this Part or for a criminal offence).

These permitted cyber security purposes have been precisely limited to those circumstances where Government needs to share and use information to address a significant cyber security incident, engage in incident response, or mitigate consequences following from an incident. These include, but are not limited to, sharing to and use by:

- law enforcement to provide them with sufficient information to investigate the perpetrator;
- the sanctions office in the Department of Foreign Affairs and Trade or the Minister for Home Affairs to ensure they have sufficient information to consider the imposition of “cyber sanctions”;
- State and Territory cyber security agencies, to perform their important functions in resolving the cyber security incident within that jurisdiction; or
- a Commonwealth or State body essential to the stability of a particular sector, such as energy markets or financial markets.

Limited use process diagram



While the Coordinator can disclose information to Commonwealth enforcement bodies in certain circumstances, there are strict limitations. The Coordinator must not make a record of, use or disclose information for the purposes of investigating or enforcing, or assisting in the investigation or enforcement of, any contravention by an impacted entity of a Commonwealth, state or territory law, other than:

- a contravention by the impacted entity of Part 4 of the *Cyber Security Act 2024*, or
- a contravention by the impacted entity of a law that imposes a penalty or sanction for a criminal offence, though that information is not admissible in criminal proceedings (except for certain proceedings relating to *Cyber Security Act 2024)* against that entity. Further detail is under the heading admissibility below.

What if it's not a significant cyber security incident? What if I think it's a significant incident but it turns out not to be?

Your information will still be captured by the limited use obligation.

If you provide information in relation to an incident that is not a cyber incident, or is a cyber incident but is not significant, all of the relevant protections still apply.

The Coordinator may make a record of, use or disclose the information to direct you to other services that may assist you to respond to, mitigate, or resolve the incident.

If it is a cyber security incident, but not a significant cyber security incident, the Coordinator can make a record of, use or disclose the information to:

- coordinate the whole-of-government response where the Coordinator considers it necessary, or
- inform and advise Ministers of the Commonwealth about the cyber security incident.

What can't be done with limited use information?

In addition to the permitted cyber security purposes, the limited use obligation places some additional protections and restrictions on the information.

Admissibility

Information provided under limited use is **not admissible** in proceedings against an impacted entity for criminal (except for certain proceedings relating to *Cyber Security Act 2024)* or civil proceedings for a contravention of a civil penalty (except civil penalties under Part 4 of the *Cyber Security Act 2024*), or for a breach of any other law (including common law), or the proceedings before a tribunal. There are exceptions, including for coronial inquiries and royal commissions, due to the significant sensitivity and gravity of those proceedings.

Legal professional privilege

The fact that an entity voluntarily provides information to the Coordinator under limited use does not otherwise affect a claim of **legal professional privilege**, under any Commonwealth, state or territory law, or before a tribunal. There are exceptions, including for coronial inquiries and royal commissions, due to the significant sensitivity and gravity of those proceedings.

Non-compellability

The measures also provides that in certain circumstances, the Coordinator (including staff members of the Coordinator) are **not compellable as witnesses** in relation to limited cyber security information in civil or criminal proceedings, of a federal court or a court of a state or territory, in relation to limited use information. In such circumstances, this ensures that the Coordinator or staff members with access to limited use information are not otherwise able to be compelled to disclose this information, such as in class-action proceedings.

Disapplication of Freedom of Information Act 1982

The *Freedom of Information Act 1982* has been amended to **exempt limited use information from freedom of information requests**. This ensures that limited use information is not able to be obtained by entities through other channels.

Not a 'safe harbour'

While the protections provided to information under limited use are quite broad, it is important to note that limited use is **not a 'safe harbour'**. This means that an entity that provides information is not shielded from legal liability just because they disclosed information to the Coordinator. While there are restrictions on using and sharing limited use information for regulatory action and such information is generally not admissible in proceedings against the entity, regulators can use their own powers to independently request information from the entity. Additionally, limited use does not in any way affect an entities existing regulatory reporting requirements.

When the protections do not apply

The Act does not prohibit the recording, use or disclosure of information if the information:

- was provided by, or on behalf of, the impacted entity to the Commonwealth about the cyber security incident to comply with certain reporting requirements
- has been provided voluntarily to the Coordinator by, or on behalf of, the impacted entity other than under Part 4 of the *Cyber Security Act 2024*, or
- has already been lawfully made available to the public.

This does not constitute an authorisation for the recording, use or disclosure of information. However, if the Coordinator or other entity is authorised under this or another law to record, use or disclose the information for certain purposes, limited use will not prohibit the Coordinator or other entity from doing so.

How does this relate to the limited use obligation for ASD?

Division 1A, Part 6 of the *Intelligence Services Act 2001* (IS Act) provides a parallel limited use obligation for the Australian Signals Directorate (ASD). While the regimes are largely similar, the limited use obligation recognises the distinct role and function of ASD for cyber security incidents. ASD is the first point of contact for entities experiencing a cyber security incident. ASD's role includes advice in relation to vulnerabilities and potential incidents as well as providing assistance after a cyber security incident has occurred.

The IS Act has almost identical protections for information provided to ASD, to encourage proactive and detailed engagement from industry with ASD in relation to a cyber security incident. You can find more information on the limited use obligation as it applies to ASD at www.cyber.gov.au.

Scenario 1- significant cyber security incident

Company X is a major telecommunications provider that has been affected by a cyber security incident where a threat actor gained access to their internal systems. Company X reports this incident via ASD's ReportCyber online reporting portal. After an unsuccessful ransom demand, the threat actor published the personal information of millions of Australians on the dark web, including drivers' licences and passport information used for identity verification.

Company X also contacts the National Office of Cyber Security (NOCS) directly to request coordination and consequence management assistance. Company X provides a briefing to assist the NOCS to understand the extent of the incident and the stakeholders that will need to be engaged in coordination activities. This information provided to the NOCS is captured by limited use because it has been provided voluntarily by an entity carrying on a business in Australia (this company is also captured as they are a responsible entity for a critical infrastructure asset), and the information is about an incident that has had an impact on the entity. That means that information provided to the NOCS is not admissible in most criminal or civil proceedings for contravention of a civil penalty provision (except under Part 4) against the impacted entity, there is no impact to any legal professional privilege that may attach to the information and the information can only be shared for permitted cyber security purposes.

Following the initial briefing, the NOCS leads a coordination call with Company X and relevant Australian Government and state and territory government agencies. The briefing, and subsequent ongoing engagement, provides an overview of the incident, considers its potential impacts and discusses the requirement for coordinated consequence management activity. The information discussed at the briefing has been shared with attendees for a permitted cyber security purpose and therefore is captured by the limited use obligation

Customers of Company X reside in all states and territories. In order to address the compromise of driver's licences and passports, the NOCS organises a working group meeting that includes state and territory cyber response agencies and licence issuing bodies so that these agencies can understand the breadth of the incident, the impact this may have on their respective jurisdictions and any particular processes they may need to put in place to manage the replacement of hundreds and thousands of driver's licences. This working group also includes representatives of the relevant Australian Government credential issuing bodies to manage the impact this incident may have on these credentials. The NOCS is able to disclose information about the incident to these agencies because it is for a permitted cyber security purpose, namely the performance of the functions of a state body responding to a cyber security incident or the performance of the functions of a Commonwealth body responding to a cyber security incident. This information will continue to hold the information protections afforded under the limited use provision, even once shared. These agencies, once in receipt of this information, will only be able to use or disclose the information for permitted cyber security purposes.

Company X separately contacts its regulators within the telecommunications sector, providing required information to acquit their regulatory responsibilities. The Coordinator is not permitted to disclose information to regulators or law enforcement agencies for the purposes of investigation or legal proceedings, unless an exception applies. Any information provided by Company X to regulators or law enforcement agencies is not covered by the protections under limited use, even where it is the same information that has been provided to the Coordinator. Company X successfully acquits their regulatory reporting obligations, and receives the assistance of the NOCS to coordinate incident response and management.

Scenario 2 – cyber security incident

Company A is a large financial services provider which has recently detected malware in their internal servers. The company has notified ASD's ACSC of a cyber security incident via the ReportCyber portal and has also contacted the NOCS. Company A notes that their initial assessment of the incident suggests only low-risk internal corporate information has been accessed, there is no sign of exfiltration and they have subsequently secured their systems.

The NOCS contacts the entity and receives a briefing on the situation. The NOCS suggests that Company A also reports the incident as a cybercrime to law enforcement via the ReportCyber portal. As no coordination or consequence management is required, no further action is taken, though the NOCS remains on standby should the situation change.

The information relating to the incident is still covered by limited use even though the incident is not "significant". If an entity provides information in relation to an incident that is not a cyber incident, or is a cyber incident but is not significant, all of the relevant protections still apply. That means it is not admissible in criminal or civil proceedings for contravention of a civil penalty provision (except under Part 4) against the impacted entity, there is no impact to any legal professional privilege that may attach to the information (with a couple of exceptions) and the information can only be shared for certain purposes.

A week later, Company A realises that the affected server contains a small amount of personal data because files relating to a state-based subsidiary have mistakenly been saved to the wrong location. As a result, several thousand residents of that state have had their personal information accessed and exfiltrated. Company A contacts the NOCS for assistance in managing this development.

In consultation with Company A, the NOCS coordinates a briefing with the company, relevant Australian Government agencies and the state government's cyber response agency. The briefing provides an overview of the incident and considers its potential impacts and consequences. Given the number of affected individuals and their location within a particular state, that state government is best placed to assist Company A and the NOCS ceases its involvement in the incident, pending any change in the impact of the incident.

The NOCS is able to disclose information about the incident to the state government because it is for a permitted cyber security purpose, that is, the performance of the functions of a state body responding to a cyber security incident. This information will continue to hold the same information protections, even once shared. The state government will only be able to use or disclose the information for permitted cyber security purposes.

Company A separately contacted regulators to fulfil their regulatory obligations.