Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Protected Information
Industry guidance for critical infrastructure assets

Contents

What is 'protected information'? 2

Why are there information sharing provisions in the Act? 2

'Harms-based' approach 3

Table: Examples of documents or information which may meet the definition of protected information 4

Disclosure of 'protected information' 5

- **Disclosure to perform a function or duty under the Act** 5
- **Disclosure for emergency management** 5
- **Disclosure of protected information by the entity to whom the information relates** 6
- **Secondary Disclosure** 7

Exceptions to the unauthorised recording, use or disclosure of protected information 8

Further information 8

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au | CISC on X, Instagram and LinkedIn

March 2025

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Protected Information
Industry guidance for critical infrastructure assets

This guidance material has been prepared to assist entities to understand what protected information is and in what circumstances it can be used or disclosed. As an Industry Partner, you must understand your responsibilities, and the limitations for sharing information with other entities.

What is 'protected information'?

In meeting their obligations under the *Security of Critical Infrastructure Act 2018* (SOCI Act) entities will record, obtain and generate information. Some of this information may be '**protected information**' under the Act. *The Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* simplified the protected information provisions in the Act by introducing an amended 'harms-based' approach to protected information. The Act also provides a non-exhaustive list of 'relevant information' to assist entities to determine if certain information is protected.

Section 5A of the Act defines 'protected information' as it applies to **critical infrastructure assets:**

*Protected information is **relevant information**:*

(a) the disclosure of which would or could reasonably be expected to prejudice national security or the defence of Australia; or

(b) the disclosure of which would or could reasonably be expected to prejudice the social or economic stability of Australia or its people; or

(c) that contains, or is, confidential commercial information; or

(d) the disclosure of which would or could reasonably be expected to prejudice the availability, integrity, reliability or security of a critical infrastructure asset.

Why are there information sharing provisions in the Act?

Certain information related to exercising powers, or performing duties or functions, under the Act may be **commercial-in-confidence or sensitive** for national security reasons.

Potential consequences of disclosure of this information can be severe. It could result in significant interruption to your business or operations, or provide hostile parties opportunities to exploit or interfere with our national security.

The revised definition of 'protected information' clarifies when and how entities can share relevant information. However, strong protections remain. **Section 45** of the Act creates an offence to record, use or disclose protected information. Authorisations and exceptions to the offence under **Sections 41 – 44** have been designed to ensure relevant entities and certain other persons can lawfully disclose and use protected information. These are described from page 5.

Relevant information is defined in Section 5A of the SOCI Act as:
(a) a document or information that is obtained or generated by a person in the course of exercising powers, or performing duties or functions, under this Act; or
(b) a document or information that is obtained, generated or adopted by an entity for the purposes of complying with this Act.
The definition provides a non-exhaustive list under Section 5A(3) of 'relevant information', which may meet this definition.

My entity handles governments documents marked 'PROTECTED' – is this the same?

The meaning of **protected information** under the SOCI Act **is not** the same or equivalent to the **PROTECTED** security classification within the Protective Security Policy Framework that may be used on Australian Government information.

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au | CISC on X, Instagram and LinkedIn

March 2025

There will be scenarios where protected information contains **confidential commercial information**.
Confidential commercial information is defined in Section 5 of the SOCI Act:
(a) information relating to trade secrets;
(b) other information that has a commercial value that would be, or could reasonably be expected to be, destroyed or diminished if the information were communicated.

'Harms-based' approach

Previously, protected information provisions in the SOCI Act were designed to apply strict information sharing restrictions on private entities operating critical infrastructure assets. Entities found those provisions hard to navigate, so recent amendments to the Act have changed the definition in favour of a **harms-based information sharing approach**.

Entities are now only prohibited from sharing '**relevant information**' that also satisfies the definition of '**protected information**'. This includes information that could **cause harm**, or **pose risk** to:

- The social or economic stability of Australia or its people
- The availability, integrity, reliability or security of a critical infrastructure asset
- Commercial interests
- National security interests
- The defence of Australia

There may be situations in which it is preferable for protected information to be disclosed or used in some way to avoid these harms or risks.

Section 42AA of the SOCI Act legislates the harm-based approach, permitting entities to make a record of, use or disclose protected information if that record, use or disclosure is:

- *for a purpose relating to the continued operation of the critical infrastructure asset; or*
- *to mitigate a risk to the availability, integrity, reliability or security of the critical infrastructure asset.*

In these circumstances, disclosure is permitted to avoid potential harm to the asset, including in time sensitive or emergency situations.

This change has been made in response to feedback from both government and industry that the previous definition may have, in some instances, unnecessarily limited the ability of Government, responsible entities and their employees to use or disclose information in the course of ordinary business, or mitigate relevant risk effectively. These changes strike a balance between having appropriate information protections in place and facilitating sharing in support of security and resilience outcomes.

A **harms-based assessment** should be used to determine if the disclosure of protected information by an entity is permitted. It considers the potential harm of disclosing relevant information about a critical infrastructure asset in determining if it should be classed as protected information, and therefore subject to non-disclosure obligations.

The balance of harm that might eventuate between disclosure and non-disclosure must be considered in this assessment. If the potential harm of not disclosing the information outweighs the potential harm of disclosing it, the disclosure and use of the information will be permitted.

Entities are expected to engage with independent or legal advice to support their harms-based assessment.

Each decision about the **disclosure** of **protected information** will turn on the relevant facts of the situation.

- *What information is being provided?*
- *Who is disclosing the information?*
- *Who is the information being disclosed to?*
- *For what purpose is the information being disclosed?*

These key factors **should always** be considered when disclosing **protected information**.

Personal Information

To ensure the protected information provisions in the SOCI Act continue to operate in harmony with the *Privacy Act 1988*, disclosure of personal information will continue to be limited to circumstances where it is necessary and for an authorised purpose.

Where protected information contains personal information, disclosure will only be permitted where it is for a specified purpose and authorised by either a specific provision or in accordance with a direction issued under the SOCI Act, or otherwise authorised by law.

Examples of information which may meet the definition of protected information

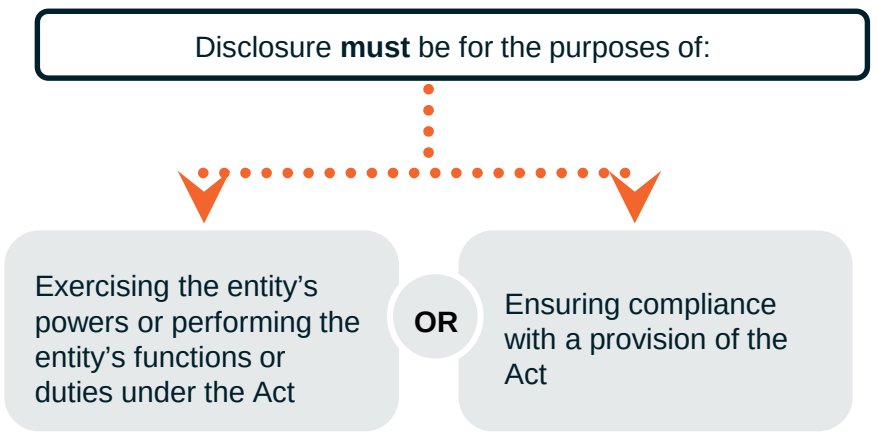
Protected Information (PI) Type	When PI can be shared under s42AA	When PI cannot be shared
Information produced in the course of **exercising powers** under the Act or **performing duties or functions** under the Act.	A construction company needs to know the location of a critical telecommunications asset (underground cable) before commencing digging works. The location is included in the asset registration and can be shared to prevent the company striking it and disrupting services (including design and engineering stages of a construction project).	The Board of a listed responsible entity is reviewing a CIRMP Annual Report. Details of the CIRMP cannot be included in publicly available minutes of that meeting.
A written declaration or **record confirming an asset is a CI asse**t under section 51.	A Ministerial declaration of a critical water asset can be provided to a sewerage servicing contractor to evidence that asset's status to prevent it from being disrupted during a prolonged maintenance period.	A law firm would like access to records of which assets have been declared CI assets, so they can approach the responsible entities to provide legal advice on complying with their obligations.
A written declaration or **record confirming an asset is a System of National Significance (SoNS)** under section 52B.	The Australian Border Force (ABF) Commissioner may require a list of SoNS to know which systems involved in the movement of goods and people are most critical to protect in case of unauthorised activity at border entry points.	A University would like to know what banking systems have been declared SoNS to inform the development of a new course on cyber security in the financial sector.
A written declaration or record that **a Ministerial authorisation has given or revoked** for the purposes of section 35AB.	A Ministerial authorisation to the Home Affairs Secretary may need to be shared with the Secretary of Defence so they are aware of information relating to the availability of a critical health asset at a Defence base.	An entity subject to an authorisation would like to share that record with the company providing their IT services so they have advanced knowledge of any system changes they may encounter.
A **critical infrastructure risk management program** (CIRMP) (or information contained therein).	The Australian Prudential Regulatory Authority (APRA) requires a critical financial services entity's CIRMP to assess compliance with a security obligation.	A labour hire firm would like to see a selection of entities' CIRMPs to better understand the security processes its clients may go through when applying to work in a CI entity.
An annual report (or information contained therein) **relating to a CIRMP.**	A cyber incident has impacted an entity's assets, and its IT provider requires access to the CIRMP to support the entity in deploying its harm minimisation processes relating to their computer systems.	A potential foreign investor wants to review an entity's CIRMP to assess its risk profile.
A **Mandatory Cyber Incident Report** (MCIR).	The Secretary of Defence needs to know the details of a cyber incident, as the affected entity supplies services to a Defence Prime.	A shareholder in an entity that experienced a cyber incident would like to know which of its goods or services have been materially disrupted to inform their investment decisions.
Reports relating to **Enhanced cyber security obligation**s for SoNS under sections 30CD, 30CQ, 30CR, 30CZ, 30DB or 30DC.	A regulated entity who is not a SoNS has assets that form part of system with SoNS assets. The regulated entity seeks to review the outcomes of the SoNS' cyber security exercise so it can prepare to support a response in the event of a compromise.	A State Employment Minister would like to see a SoNS' incident response plans to project what kinds of skills will be required in the future to respond to emerging risks to CI assets in their State.
Secretary's directions or requests issued under section 35AK, 35AQ or 35AX.	Information provided to the Secretary from an entity about an incident can be provided to a State Police Minister to inform a related transnational crime operation.	A news reporter would like to gather information on how the Secretary's powers are being used under the Act to inform an upcoming story.

Disclosure of 'protected information'

The following sections detail where protected information is allowed or required to be disclosed, in addition to those reasons allowed for under Section 42AA.

Disclosure to perform a function or duty under the Act (Section 41)

Section 41 is a general authorisation to enable an entity to record, use or disclose protected information to **comply with the Act** or **exercise a power** or **perform its relevant functions or duties** under the Act.



Whether an entity is exercising a **power** or performing a **function** or **duty** under the Act will depend on the circumstances of the situation. In general terms, an entity will:

- exercise a **power** where an authority is conferred onto them under the Act.
- perform a **function** where they are acting with a purpose which has been assigned to them under the Act.
- perform a **duty** where they are complying with an obligation. This includes a **duty** for a position or occupation designated within the Act.

Example – Disclosure to boards / directors to comply with the Act

A responsible entity has adopted and is currently maintaining a CIRMP in accordance with the requirements of Part 2A of the Act.

The responsible entity is required to submit an annual report on the CIRMP for the financial year. Under section 30AG the annual report must be approved by the board, council or other governing body of the entity.

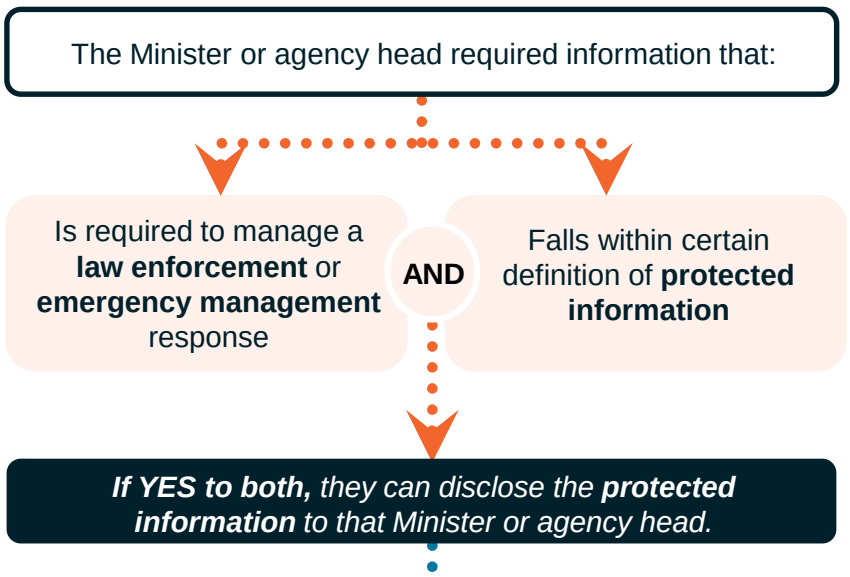
To comply with this requirement, the responsible entity must disclose **protected information** about the **CIRMP** of the asset to the Board, Directors or external Directors.

A disclosure of **protected information** in these circumstances would be authorised under **section 41** of the Act.

Disclosure for emergency management (Section 42(2))

Section 42(2) gives the Secretary the power to disclose protected information to a Commonwealth, State and Territory Minister, agency head, or member of their staff, where the Minister or agency is responsible for emergency management, law enforcement or the regulation of the critical infrastructure sector to which the protected information relates.

This provision recognises the role such a Minister may play in responding to a serious incident impacting critical infrastructure.



Example – Disclosure for emergency management

A natural disaster has occurred in Queensland. The State Minister for Police and Emergency Services requires access to **protected information** relating to the nature of critical infrastructure assets to coordinate the disaster response.

The Secretary can disclose this information to the Minister, so long as the disclosure for the same purpose for which the Minister initially obtained the information (i.e. the disclosure is to enable the State Minister's response to an ongoing natural disaster).

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Disclosure of protected information by the entity to whom the information relates (Section 43E)

Section 43E provides for two circumstances in which protected information can be disclosed by an entity, when the information relates to that entity.

Subsection 43E(1) provides authorisation for an entity to disclose protected information relating to itself to:

- A Minister of the Commonwealth, a State, the Australian Capital Territory or the Northern Territory who has responsibility for the regulation or oversight of the relevant critical infrastructure sector to which the protected information relates;
- A person employed as a member of staff of a Minister mentioned above; or
- The head of an agency (including a Department) administered by the Minister mentioned above; where the disclosure is for the purposes of enabling or assisting them to exercise their powers or perform their functions or duties (e.g. for regulatory purposes).

Who can the information be disclosed to?

Minister of the Commonwealth with responsibility for a critical infrastructure sector (or staff)

OR

Minister of a State or Territory with responsibility for a critical infrastructure sector (or staff)

OR

Head of an agency administered by a Minister with responsibility for a critical infrastructure sector (or officer)

If YES to any, *you may disclose the* ***protected information*** *where the purpose of disclosure is to:*

Enable or assist the recipient to exercise their powers or perform their functions or duties

Subsection 43E(1) Example – Disclosure to a State or Territory Minister for the purpose of exercising a power

A responsible entity for a critical public transport asset proposed to share a **mandatory cyber incident** report made under **Section 30BC** with the Minister for Transport for NSW.

The specific written report contains details on an ongoing critical cyber security incident impacting one of the entity's critical infrastructure assets. The report would fall within definition of **protected information** and the relevant Minister has oversight of the transport sector in NSW.

The purpose of disclosing this report is to enable or assist the Minister to exercise their **powers** or perform their **functions** or **duties** under the relevant state-based legislation.

In this case, the disclosure will likely be authorised by **section 43E(1)**.

Subsection 43E(2) allows entities to **seek the consent of the Secretary of Home Affairs** to disclose certain protected information for commercial requirements or other reasons not contemplated and authorised by the Act.

Given the improper disclosure of protected information could have unintended negative consequences, it is necessary to obtain the Secretary's consent for the disclosure of this information.

The Secretary's consent may be subject to one or more conditions which must be satisfied prior to the disclosure of the protected information.

The information an entity needs, or is required, to disclose is information that:

Relates to the entity itself

AND

Falls within the definition of **protected information**

If YES to both, *you may request the Secretary's written consent to disclose the* ***protected information****.**

The Secretary must consent to the disclosure in writing

AND

Any conditions imposed must be satisfied (where applicable)

*If a responsible entity wishes to seek the Secretary's consent, please contact enquiries@CISC.gov.au

Subsection 43E(2) Example – Disclosure of a SoNS declaration

An asset of a responsible entity (**Entity A**) has been declared a System of National Significance (**SoNS**) under **section 52B** of the Act.

A **SoNS declaration** falls into the class of **protected information**.

If **Entity A** wanted to disclose the **SoNS declaration** to a potential investor (**Entity B**), **Entity A** could apply to the Secretary (or delegate) for written consent to disclose this information to **Entity B**.

If the Secretary or delegate's consent is given, the protected information may be disclosed to **Entity B**.

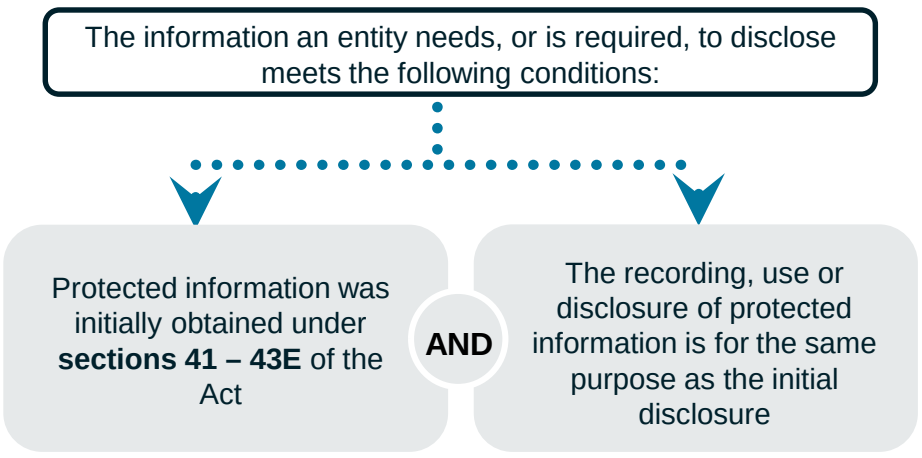
Entity B may then use or disclose the protected information in accordance with **section 44** (see below).

This disclosure may be subject to conditions as outlined by the Secretary.

Secondary Disclosure (Section 44)

Under **Section 44** of the Act, if an entity has obtained **protected information** under one of the authorised use and disclosure provisions in the Act (**Sections 41 – 43E** of the Act), the information can be recorded, used or disclosed to a secondary entity for the same purpose that it was obtained by the entity.

Whether a disclosure is for the same purpose for which the information was initially received will depend on the circumstances of the situation.



Example – Secondary disclosure of security report to an academic

A cyber security consulting firm has received a report from a responsible entity of a **CI asset** under **section 41**. The report was disclosed to allow the consulting firm to provide advice regarding an emerging cyber security threat.

This threat represents a material risk to the CI asset and is not adequately considered within the processes established and maintained by the responsible entity in accordance **with section 8** of the **CIRMP Rules**. This advice will inform how the responsible entity should update its processes to secure the **CI asset.**

In this instance, the consulting firm may choose to disclose the report to a noted cyber security academic who has specific expertise on this issue.

The firm is disclosing the **protected information** for the same reason they received the information under **section 41** (i.e. providing advice to the responsible entity).

In this example, the disclosure may be authorised under **Section 44.**

Exceptions to the unauthorised recording, use or disclosure of protected information

If an entity is not authorised to make a record of, disclose or otherwise use **protected information**, consideration could be given to whether an exception to the offence in **Section 45** may apply.

In addition to any exceptions that might be made under Section 42AA, **Section 46** of the Act provides four exceptions, listed below.

1. The use or disclosure is required or authorised by law

Under **subsection 46(1)**, the offence in **section 45** does not apply if the making of the record, or the disclosure or use of the information is required or authorised by or under:

- a law of the Commonwealth, other than subdivision A (**sections 41 – 44** of the Act) or a **notification provision**;[1] or
- a law of a State or Territory prescribed by the rules.[2]

2. The use or disclosure was in good faith and in purported compliance with Subdivision A or a notification provision

Under **subsection 46(3)**, the offence in **section 45** does not apply to an entity to the extent that the entity makes a record of, discloses or otherwise uses **protected information** in good faith and in purported compliance with:

- subdivision A (**sections 41 – 44** of the Act); or
- a **notification provision** (see **section 5** of the Act).

3. The use or disclosure is to, or with the consent of, the entity to whom the protected information relates

Under **subsection 46(4)**, the offence in **section 45** does not apply to an entity if:

- the entity discloses **protected information** to the entity to whom the information relates; or
- the making of the record, or the use or disclosure of the **protected information** is done in accordance with the express or implied consent of the entity to whom the **protected information** relates.

4. The use or disclosure is to an Ombudsman official

Under **subsection 46(5)**, the offence in **section 45** does not apply to an entity to the extent that the entity discloses **protected information** to an Ombudsman official for the purposes of exercising **powers** or performing **duties** or **functions** as an Ombudsman official.

Further information

Who should I contact if I have further questions about protected information?

If you are an entity, including a business, and you believe you have a need to record, use or disclose **protected information** you can contact the CISC at enquiries@CISC.gov.au.

Can the Department of Home Affairs freely share my information?

No. The Government must also comply with **protected information** use and disclosure provisions as well as any other applicable laws relevant to handling of the information.

Where can I find further resources for critical infrastructure?

More information on the protection of Australia's critical infrastructure can be found on the CISC's website.

The key **legislative instruments** are listed below and can be found here:

- Security of Critical Infrastructure Act 2018
- Security of Critical Infrastructure (Critical infrastructure risk management program) Rules
- Security of Critical Infrastructure (Application) Rules
- Security of Critical Infrastructure (Definitions) Rules

A summary of useful information and guidance about SOCI obligations can be found on the fact sheet page of the CISC's website.

Please note that CISC can provide general information but cannot provide legal advice.

---

[1] For the purposes of this exception, the following laws:
(a) the Corporations Act 2001, except a provision of that Act prescribed by the rules;
(b) a law, or provision of a law, of the Commonwealth prescribed by the rules;
are taken not to require or authorise the making of a record, or the disclosure, of the fact that an asset is declared under **Section 51 to be a critical infrastructure asset** or of the fact that an asset is declared under **Section 52B to be a system of national significance**.

[2] As of the publication of this guidance material, no rules have been made for **paragraph 46(1)(b)** of the Act.