Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

CONSULTATION DRAFT v1

Protected Information

Guidance Material – Industry

As at 9 September 2022

Contents

1. Why are there information sharing provisions in the Act?

- The *Security of Critical Infrastructure Act 2018* (the Act) sets out a framework for the sharing of protected information in certain circumstances.
- The protected information provisions in the Act have been designed to facilitate the recording, use or disclosure of information by a responsible entity for a critical infrastructure asset(s) in a range of circumstances to ensure they can comply with their obligations under the Act.

2. What is 'protected information'?

- Section 5 of the Act sets out the definition of **protected information**. The following table provides a summary of the types of documents or information that constitutes protected information under the Act. **Please note:** protected information in the Act **is not** the same as the **PROTECTED** security classification, or any other classification, in the **Protective Security Policy Framework**.

Protected information means a document or information that:	Act Reference
Is obtained by a person in the course of exercising powers, or performing duties or functions, under this Act	5(a)
Records or is the fact that an asset is privately declared under section 51 to be a critical infrastructure asset	5(b)
Records or is the fact that an asset is privately declared under section 52B to be a system of national significance	5(ba)
Records or is the fact that the Minister has: • given a Ministerial authorisation; or • revoked a Ministerial authorisation	5(bb)
Is (or is included in) a critical infrastructure risk management program that is adopted by an entity in compliance with section 30AC	5(bc)
Is (or is included in) an annual report relating to the risk management program obligation given under sections 30AG or 30AQ	5(bd)
Is (or is included in) a report about a critical cyber security incident under sections 30BC or other cyber security incident under 30BD	5(be)
Is (or is included in) an incident response plan adopted by an entity in compliance with section 30CD	5(bf)
Is (or is included in) an evaluation report in relation cyber security exercises under section 30CQ or 30CR	5(bg)
Is (or is included in) a vulnerability assessment report under section 30CZ	5(bh)
Is (or is included in) a report prepared in compliance with: • a system information periodic reporting notice under section 30DB; or • a system information event-based reporting notice under section 30DC	5(bi)
Records or is the fact that the Secretary has: • given an information gathering direction or request under section 35AK; or • revoked such a direction or request	5(bj)
Records or is the fact that the Secretary has: • given an action direction or request under section 35AQ; or • revoked such a direction or request	5(bk)
Records or is the fact that the Secretary has: • given an intervention direction or request under section 35AX; or • revoked such a direction or request	5(bl)
A document or information listed above that is obtained by a person by way of an authorised disclosure under the Act or in accordance with an exception listed in section 46 of the Act.	5(c)

3. Disclosure of protected information – commercial and compliance purposes

- The protected information provisions in the Act have been designed to facilitate the recording, use or disclosure of information by a responsible entity for a critical infrastructure asset(s) in a range of circumstances.

STOP

Each decision about the disclosure of protected information will turn on the relevant facts in the situation, including the information that is being disclosed, who is disclosing the information, who the information is being disclosed to and for what purpose the information is being disclosed. Consideration should always be given to these factors when making a decision about the disclosure of protected information.

- The following tables provide an overview of the key authorisations and exceptions under the Act that you may consider when:
  - seeking to disclose protected information to **external parties**, such as lawyers, security consultants and insurance professionals, for compliance purposes;
  - seeking to disclose protected information to **related bodies corporate** for commercial purposes;
  - seeking to disclose protected information to **boards, directors or external directors** for corporate and governance purposes

Relevant authorisation – section 41			**Act reference**
Performing functions or duties under the Act	*Who can disclose?*	an **entity** (defined in **section 5** of the Act)	S 5
	What can be disclosed?	protected information (see **section 2**)	S 5
	Who can the information be disclosed to?	other parties (complying with the **conditions of disclosure**)	S 41
	Conditions of disclosure?	the disclosure must be for the purpose of: - exercising the entity's **powers** or performing the entity **functions or duties** under the Act; or - ensuring compliance with a provision of the Act	S 41(a)-(b)
	Is secondary disclosure available?	yes – see section 44	S 44

Example 1 – disclosure to lawyers and consultants for the purpose of complying with the Act

The responsible entity for a critical gas asset is unsure if their current risk management program is compliant with the requirements set out in the critical infrastructure risk management program rules made under the Act.

Under **section 41** of the Act, the responsible entity may be authorised to disclose protected information about the detail of their risk management program to an external party, such as a legal practitioner or a security consultant, **for the purpose of** seeking advice on whether they are compliant with the risk management program obligation.

- **Section 41** is a general authorisation to enable an entity (including a body corporate or politic) to record, use or disclose protected information in order to comply with the Act and perform its relevant functions or duties as required under the Act.
- Compliance with certain provisions of the Act may require the sharing of protected information with boards and directors of critical infrastructure assets, such as:
  - **section 30AG** – responsible entity must submit an annual report;
  - **section 30AQ** – reporting obligations relating to certain assets that are not covered by a critical infrastructure risk management program
- If the recording, use or disclosure of protected information to the board, director or external director is required in order to ensure compliance with a provision under the Act, it may be authorised under **section 41**.

Example 2 – disclosure to boards/directors for the purpose of complying with the Act

The responsible entity for a critical data storage or processing asset has adopted and is currently maintaining a critical infrastructure risk management program in compliance with the requirements of **Part 2A** of the Act.

As part of the annual reporting requirement in **section 30AG** of the Act, the responsible entity is required to submit a report on the risk management program for a financial year that is approved by the board, council or other governing body of the entity.

To comply with this requirement and ensure the accuracy of the report, this may require the disclosure of protected information about the detail of a risk management program of the asset to the board, directors or external directors.

Relevant authorisation – subsection 43E(2)			Act reference
Authorised disclosure at the Secretary's written consent	*Who can disclose?*	an **entity** (defined in **section 5** of the Act)	S 5
	What can be disclosed?	protected information (see **section 2**) that: - **relates to itself**; and - is covered by paragraphs (b)-(bl) of the definition of protected information	S 43E(2)(i)
	Who can the information be disclosed to?	other parties (complying with the **conditions of disclosure**)	S 43E(2)(b)(iii)-(iv)
	Conditions of disclosure?	the Secretary must **consent** to the disclosure. If the Secretary's consent is subject to one or more **conditions**, those conditions must be satisfied	S 43E(2)(b)(iii)-(iv)
	Is secondary disclosure available?	yes (**subject to the Secretary's conditions**) – see section 44	S 44

- The purpose of **subsection 43E(2)** is to provide an entity with flexibility to seek the Secretary's consent to disclose specified **protected information** for commercial requirements or other reasons not contemplated and already authorised by the Act.
- Given the sensitive nature of protected information, the disclosure of which may include sensitive and inherently harmful information as defined by the *Criminal Code 1995*, and the potential for harm to Australia's national interest if this information was disclosed to certain people, it is necessary to obtain the Secretary's consent for the disclosure of this information.

Example 3 – disclosure of a SONS declaration with the Secretary's written consent

A critical electricity asset of **Entity A** has been declared a System of National Significance (SONS) under **section 52B** of the Act.

Under paragraph 5(ba) of the definition of 'protected information', a SONS declaration falls into the class of protected information covered by **subsection 43E(2)**, due to the criticality of the SONS to Australia's social and economic stability, defence or national security.

In the event that **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**, subject to any conditions that may apply.

Relevant authorisation – section 44			Act reference
Secondary disclosure of protected information	*Who can disclose?*	an **entity** (defined in **section 5** of the Act)	S 5
	What can be disclosed?	protected information (see **section 2**)	S 5
	Who can the information be disclosed to?	other parties (complying with the **conditions of disclosure**)	S 44
	Conditions of disclosure?	the protected information was initially obtained under **sections 41-44** of the Act; and the recording, use or **disclosure** of protected information is for the **same purpose** as the initial disclosure	S 44
	Is secondary disclosure available?	yes – see section 44	S 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 – 44 of the Act**), the information can be recorded, used or disclosed to a secondary entity for the same purpose.

Example 4 – secondary disclosure of a cyber-evaluation report to a security consultant

The Department has disclosed an evaluation report (section 30CR) to an entity (**Entity A**) in compliance with the requirements of the Act (under **section 41**). The purpose of sharing the evaluation report was to assist **Entity A** in better understanding and taking any necessary steps to ensure an asset of the highest criticality is safeguarded and secured from cyber security incidents.

On this basis, **Entity A** may be able to disclose this protected information to an **Entity B** (i.e. a cybersecurity consultant) under **section 44** of the Act for the **same purpose** of better understanding and taking necessary steps to safeguard and secure their critical asset against cyber security incidents.

Relevant exception – Paragraph 46(4)(c)			Act reference
Disclosure with the consent of the entity to whom the information relates	*Who can disclose?*	an **entity** (defined in **section 5** of the Act)	S 5
	What can be disclosed?	protected information (see **section 2**)	S 5
	Who can the information be disclosed to?	other parties (complying with the **conditions of disclosure**)	S 46(4)(c)
	Conditions of disclosure?	the making of the record, or the disclosure or use, of the protected information is in accordance with **the express or implied consent of the entity** to whom the information relates.	S 46(4)(c)
	Is secondary disclosure available?	no – section 44 does not apply to exceptions	S 44

4. Disclosure of protected information – Government purposes

- When seeking to record, use or disclose protected information for Government purposes, such as for funding or regulatory discussions, you may also consider the authorisation in **subsection 43E(1)** of the Act, **in addition to** the authorisations listed in **section 3** of this document.

Relevant authorisation – subsection 43E(1)			Act reference
Authorised disclosure by the entity to whom the information relates	*Who can disclose?*	an **entity**	S 5
	What can be disclosed?	protected information (see **section 2**) relating to the entity	S 43E(1)(a)
	Who can the information be disclosed 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; or a person employed as a **member of staff** of a Minister mentioned above; or the **head of an agency** (including a Department) administered by a Minister mentioned above, or an **officer or employee** that agency	S 43E(1)(b)
	Conditions of disclosure?	the disclosure must be for the purpose of enabling or assisting one of the people listed above to **exercise their powers or perform their functions or duties** **(not limited to powers, functions or duties under the Act)**.	S 43E(1)(c)
	Is secondary disclosure available?	yes – see section 44	S 44

Example 1 – disclosure of protected information to Government regulators for their functions

A responsible entity for a critical gas asset is required to adopt, maintain and comply with a risk management program under **Part 2A** of the Act. To comply with the obligation, the entity has been required to invest capital into uplifting its existing cybersecurity arrangements for the asset.

For the purposes of informing pricing discussions with the relevant government regulator, the entity may need to disclose detail about its risk management program (**paragraph (bc)** of the definition of **protected information**) to the energy regulator for the purpose of informing these pricing discussions.

Example 2 – disclosure of protected information to a State Minister to assist with exercising powers under state legislation

A responsible entity for a critical public transport asset proposes to share a **mandatory cyber incident report** made under **section 30BC** about a critical cyber security incident impacting one of its critical infrastructure assets (**paragraph 5(be**) of the definition of protected information) with the Minister for Transport for New South Wales. The Minister for Transport NSW has responsibility for the transport sector in their State.

The purpose of the responsible entity 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 (for example, the *Transport Administration Act 1988 (NSW)*). In this case, the disclosure could be authorised by **section 43E(1)** of the Act.

5. Exemptions to the unauthorised recording, use or disclosure of protected information?

- **Section 45** of the Act makes it an offence for an entity to make a record of, disclose or otherwise use protected information, unless the entity is authorised under the Act (**sections 41–44**) or required by a notification provision. If the entity is not authorised under the Act, an exception to the offence in **section 45** may be available to an entity. These four exemptions are listed below:

5.1 The use or disclosure is required or authorised by law

- Under **subsection 46(1)** of the Act, 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]

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

- **Under subsection 46(3)** of the Act, making a record of, disclosing or otherwise using protected information is not an offence where the disclosure is done 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).

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

- Under **subsection 46(4)** of the Act, 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.

5.4 The use or disclosure is to an Ombudsman official

- Under **subsection 46(5)** of the Act, 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.

---

[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 a 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 (09/09/2022) no rules have been made for paragraph 46(1)(b) of the Act.

6. Further information

6.1 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 Cyber and Infrastructure Security Centre at enquiries@CISC.gov.au.

6.2 Can the Department of Home Affairs freely share my information?

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