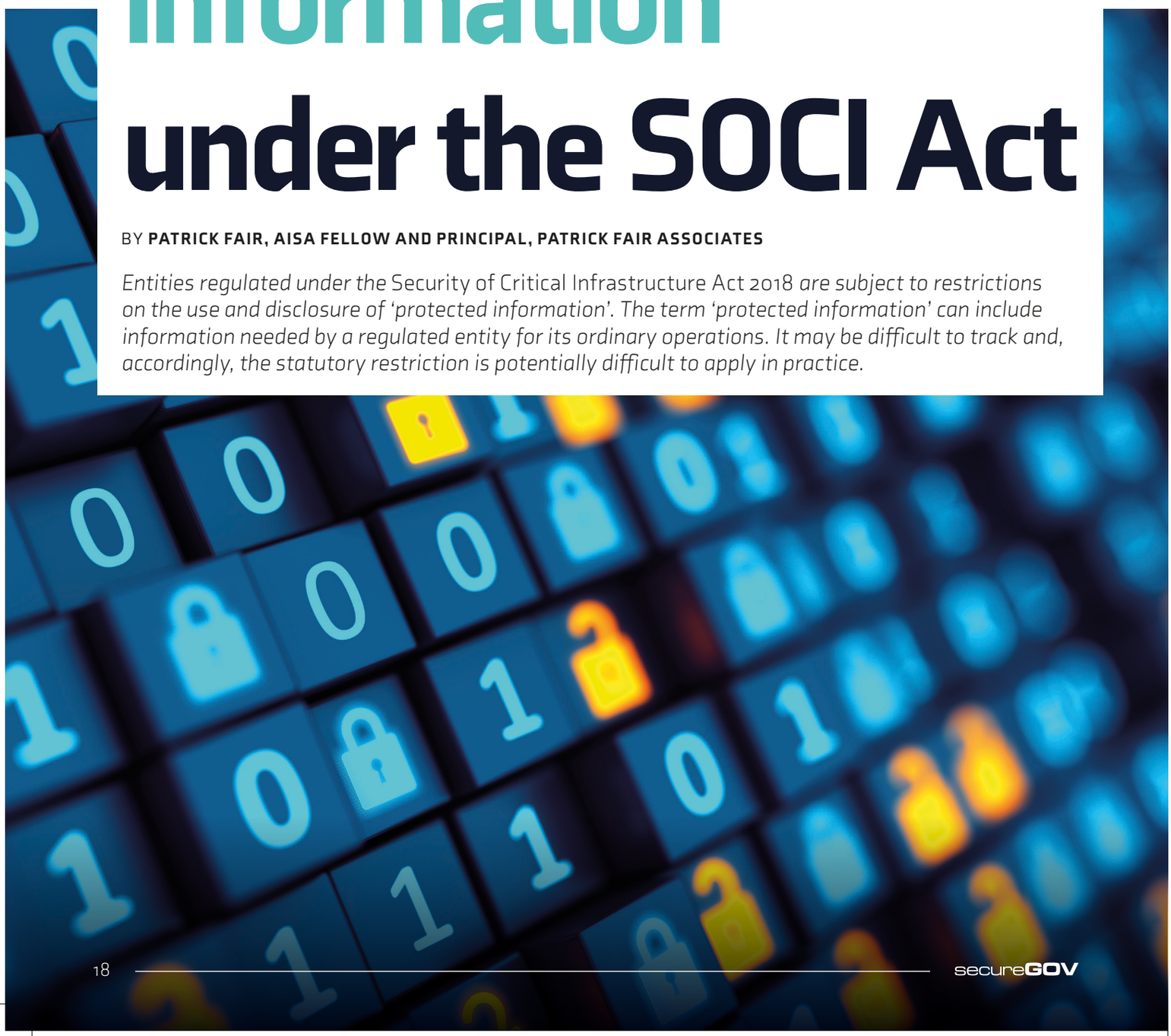
The challenge of 'protected information' under the SOCI Act

BY **PATRICK FAIR, AISA FELLOW AND PRINCIPAL, PATRICK FAIR ASSOCIATES**

Entities regulated under the Security of Critical Infrastructure Act 2018 *are subject to restrictions on the use and disclosure of 'protected information'. The term 'protected information' can include information needed by a regulated entity for its ordinary operations. It may be difficult to track and, accordingly, the statutory restriction is potentially difficult to apply in practice.*



In this short article, I set out the meaning of 'protected information' as referred to in the *Security of Critical Infrastructure (SOCI) Act 2018*, discuss the way in which the SOCI Act controls its use, and highlight the practical challenges that arise.

BACKGROUND

In March 2022, the SOCI Act was amended to cover 11 industry sectors encompassing 22 classes of critical infrastructure asset (CIA).

The changes applied ownership, control and reporting obligations across the newly regulated entities, and introduced new cyber incident reporting requirements and risk management program requirements, a process for designating Systems of National Significance (SoNS), and a range of new requirements and controls for SoNS.

The amendments expanded the meaning of protected information to cover information associated with SoNS, and made a minor change to the scope of control; however, the main impact of the changes was that the control of protected information was now legislated to be applied beyond gas, water, electricity, and ports to seven newly regulated industry sectors. These include communications, data storage and processing, financial services and markets, health care and medical, higher education and research, food and grocery, and space technology and defence.

WHAT IS PROTECTED INFORMATION?

The definition of protected information is a list of three criteria – any one of which satisfies the definition. According to Section 5 of the Act, protected information means a document or information that:

1. is obtained by a person in the course of exercising powers, or performing duties or functions, under this Act
2. records or is the fact that an asset is declared under section 51 to be a critical infrastructure asset
3. was a document or information to which paragraph (a) or (b) applied and is obtained by a person by way of an authorised disclosure under Division 3 of Part 4, or in accordance with section 46.

The first item describes a general category of documents and information.

Each of the subsequent items refers to documents or information that 'is or records' the exercise of a power of the Minister for Home Affairs or the Secretary of the Department of Home Affairs, or 'is or is included in' a document or report that must be created under the SOCI Act.

The following documents and information are (indirectly) listed or inferred from the broad first category in sub paragraph (a) of the definition:

- the power of the minister to secretly declare an asset to be a CIA
- a declaration that an asset is a SoNS
- an authorisation whereby, in the case of a serious cyber incident, the minister can authorise the Secretary of Home Affairs to give directions and make requests relating to the cyber incident and CIAs
- the risk management program required by the SOCI Act and the information it contains
- the annual report that regulated entities must file regarding their management program, that it is up to date, identifying each hazard encountered during the reporting period and providing an evaluation of the effectiveness of the risk management program in dealing with it
- the incident response plan required of a SoNS
- the internal and possibly external evaluation reports of participation in cyber security exercises required of a SoNS
- any vulnerability assessment report required of a SoNS by the Secretary of the Department of Home Affairs
- any system information periodic reporting notice required of a SoNS by a notice issued by the Secretary of the Department of Home Affairs
- any information gathering direction in relation to a cyber security incident, or an asset issued by the Secretary of the Department of Home Affairs following a Ministerial Direction
- any action direction issued by the Secretary of the Department of Home Affairs in relation to a cyber security incident or a CIA
- any intervention request issued by the Secretary of the Department of Home Affairs to the Australian Signals Directorate to do one or more specified acts

- any cyber incident reports, including the information to be set out in statutory rules, and any document containing information listed above that is created by way of a disclosure authorised under the SOCI Act.

On the final point, no rules appear to have been made at the time of writing; however, the CISC Factsheet – Cyber Security Incident Reporting says that when making a report, 'you will be asked to provide the following:

- point of contact information
- organisation information (including Australian Business Number)
- critical infrastructure sector
- the date and time the incident was identified, and whether it is ongoing
- confirmation whether the incident is having a significant impact on your asset
- details on how the incident was discovered; the nature of the incident being reported (e.g., ransomware or denial of service); whether the incident is affecting information technology, operational technology, or customer data); and whether the incident has been reported elsewhere
- any other relevant information'.

In summary, protected information includes the fact and contents of any declaration, authorisation or formal request given under the Act by the Minister for Home Affairs or the Secretary of the Department of Home Affairs. The term also covers a general category of information and certain documents with the information they contain:

- the broad and vague inclusion of 'all information obtained by a person in the course of exercising powers or performing duties or functions'. In this category would be the information collected (and information incidental to) preparing ownership and operational filings for the Register of CIAs maintained by the Secretary of the Department of Home Affairs. This category also includes entities' preparation work on creating programs and reports required by the SOCI Act. Making the Registry filings, programs and reports are 'duties' under the SOCI Act. Note that regulated entities do not appear to have any significant 'powers' or 'functions' under the SOCI Act. Powers and functions are given to the Minister for Home Affairs and the Secretary of the Department of Home Affairs. In general, the SOCI Act has duties for regulated entities
- risk management programs, annual reports on risk managing programs and cyber incident reports for regulated entities of all kinds
- incident response plans, evaluations of cyber security exercises, and vulnerability assessments for SoNS.

It is notable that the programs, reports, plans, evaluations, and assessments referred to would ordinarily contain substantive operational information necessary for the ordinary functioning of the subject CIA, and communications with the people and third parties that maintain its operation. If included, such information will become protected information.

WHAT CAN A BUSINESS DO WITH PROTECTED INFORMATION?

The SOCI Act makes it an offence for any entity to make a record of, disclose or otherwise use protected information unless the making of the record disclosure or use is authorised by the Act. The maximum penalty for breach of this obligation is $26,640 or two years in prison.

The SOCI Act authorises:

- the making of a record of, use or disclosure of protected information for the purpose of exercising powers, or performing functions or duties under the SOCI Act, or otherwise complying with the SOCI Act
- disclosure to the Minister for Home Affairs and the Department of Home Affairsand personnel
- disclosure (but not recording or use) by the entity to whom the protected information relates if the information is 'obtained by a person in the course of exercising powers, or performing duties or functions, under this Act' (i.e., information covered by the first paragraph of the definition of protected information and not covered by any other subparagraph)
- an entity that receives protected information as authorised by the SOCI Act to record, use or disclose it for the authorised purpose
- disclosures required or authorised by law
- compliance with the *Corporations Act*

2010 (except a provision prescribed by the rules)
- good faith compliance with the SOCI Act or compliance with a notification provision
- disclosure to the entity to whom the information relates
- recording, disclosure and use with the 'express or implied consent of the entity to whom the information relate'. This would protect a third party acting in good faith, but not the entity to whom the information relates (who originally disclosed the information) unless the disclosing party can identify an authorisation under which it might make the disclosure
- disclosures to the Ombudsman.

THE CHALLENGE FOR REGULATED ENTITIES

The challenge for regulated entities is how to make this framework workable.

Considering that any information included in programs, reports, plans, evaluations, or assessments cannot be recorded, used, or disclosed except to the regulator and/or for performing duties under the SOCI Act, a prudent course would be to exclude information that is ordinarily communicated and used in operations from these documents.

Accordingly:
- A risk management program should not include practical information relating to specific context. For example, a useful schema of the IT system to be protected, a plan of physical location to be subject to perimeter security, or the name and contact details of any responsible personnel.
- Notwithstanding the CISC Factsheet, it would be prudent not to include general business information in a cyber incident report (e.g., point of contact information) and, when providing information on the nature of the incident being reported and how it is affecting operational systems, not to include any details generally required for use or operation of the systems.
- If the Secretary of the Department of Home Affairs were to issue an information-gathering direction seeking operational information relating to a particular system or process, it would be prudent for the responsible entity to decline to respond until and unless the Secretary grants a statutory authorisation for the entity to continue to record, use or disclose the protected information. The Secretary has this power under Section 42 of the SOCI Act.

A key concern is that risk information from many critical infrastructure entities is fundamental to the maintenance of the longstanding 'social contract' between the community and the services to support the trust with the service delivery, and community quality and health standards. Types of such information for the water sector include information about dam safety risk and dangerous goods, where there is a need for the open sharing of risk information with all facets of community, including neighbours, local government, philanthropic organisations, and emergency services.

In addition, Australian infrastructure is at the leading edge of innovation internationally due to the infrastructure operating environment, which requires the constant drive to innovate, and this can only occur with open sharing of operational, engineering and risk information.

WHAT CAN GOVERNMENT DO WITH PROTECTED INFORMATION?

Protected information provided to the Secretary of the Department of Home Affairs can be shared with the minister with responsibility for national security, law enforcement, foreign investment in Australia, taxation policy, industry policy, promoting investment in Australia, defence, the regulation or oversight of the relevant critical infrastructure sector to which the protected information relates; a minister of a state or 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 relevant minister, the head of an agency (including a department) administered by a relevant minister, or an officer or employee of that agency; the Ombudsman; the Inspector General of Intelligence and Security; and the Australian Signals Directorate.

The potentially wide circulation of protected information within government is another reason to keep substantive system and business operation information out of

programs related to the SOCI Act, reports, plans, evaluations, and assessments.

CONCLUSION

Perhaps you are thinking that there must be an implied right to use ordinary business information in the usual way, even if it finds its way into a SOCI Act document. There are arguments that support a more practical operation of the protected information framework.

It might be argued that being a provider of a critical infrastructure asset is a 'function' under the SOCI Act and therefore use of protected information for the purposes of the asset is expressly permitted. The problem with this argument is that the SOCI Act does not prescribe any functions for regulated entities.

It might also be argued that the draftsperson intended information to be taken in context; i.e., it is protected if it is in a report but not protected when it is in routine use. The problem with this argument is that it undermines the express restrictions stated by the Act.

There is another argument that the provision that allows disclosure that takes place with 'express or implied consent of the entity to whom the information relates' implies that the person to whom the information relates has agency disclosure and, therefore, must be able to use the information as they like. The problem with this argument is that it takes the exception for disclosures to third parties out of context and ignores the express restrictions imposed on the person to whom the information relates imposed by the rest of the Act.

You might also be thinking, 'This is ridiculous! Surely this was not the intended outcome? To what good purpose would the government subject ordinary operating information (which might usefully be included in a risk management program, incident report etc.) to a prohibition on recording, use and disclosure?' Multiple submitters complained to Home Affairs, and subsequently to the Parliamentary Joint Committee on Intelligence and Security, that the protected information provisions were too restrictive and would not work in practice. Unfortunately, the few amendments made focused on facilitating the circulation of the information within government. The framework described is, perhaps, intended to help secure the regulated assets, practicality being a secondary consideration. S

The author acknowledges and thanks the Water Services Association of Australia for contributing to this article.