

SOCI Act obligations for critical aviation assets

Responsible entities for critical infrastructure assets, including critical aviation assets, have certain obligations under the [Security of Critical Infrastructure Act 2018 \(SOCI Act\)](#).

What is a 'critical aviation asset'?

There are two definitions of critical aviation asset – a broad definition in [section 5 of the SOCI Act](#), and a narrower definition in the [Security of Critical Infrastructure \(Application\) Rules \(LIN 22/026\) 2022](#) (the Application Rules).

Under section 5 of the **SOCI Act**, a critical aviation asset includes any of the following:

- an asset used in connection with the provision of an air service and is owned or operated by an **aircraft operator**;
- an asset used in connection with the provision of an air service; and is owned or operated by a **regulated air cargo agent**;
- an asset used by an **airport operator** in connection with the **operation of an airport**.

Under subsection 5(2) of the **Application Rules**, a critical aviation asset includes any of the following:

- a **designated airport**;
- an asset used to perform an Australian **prescribed air service** operating **screened air services** that depart from a **designated airport**;
- a **cargo terminal** that:
 - is owned or operated by a **regulated air cargo agent** that is also a **cargo terminal operator**;
 - and is located at a **designated airport**.

Designated airport and prescribed air service have the same meanings as in the [Aviation Transport Security Act 2004](#).

Regulated cargo agent and screened air service have the same meanings as in the [Aviation Transport Security Act 2005](#).

Cargo terminal and cargo terminal operator have the same meanings as in the [Customs Act 1901](#).

What obligations apply under the definitions?

SOCI Act obligations	Applicable to critical aviation assets?
Part 2B SOCI Act Mandatory cyber security incident reporting obligation*	Yes, for critical aviation assets as defined in the Application Rules
Subsection 12F(3) SOCI Act Notify your data storage or processing provider if it provides services on a commercial basis that relate to business critical data*	Yes, for critical aviation assets as defined in section 5 of the SOCI Act .
Part 2 SOCI Act Provide operational and ownership information to the register of critical infrastructure assets*	No
Part 2A SOCI Act Requirement to establish, maintain, and comply with a Risk Management Program*	No

*For information on these obligations and relevant compliance periods, please refer to the guidance material on the [CISC website](#).

What is the mandatory cyber security incident reporting obligation?

From 8 July 2022, **responsible entities** for critical aviation assets (as defined in the [Application Rules](#)) are required to **report cyber security incidents** to the Australian Cyber Security Centre (ACSC). This is the mandatory cyber security incident reporting obligation.

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.



SOCI Act obligations for critical aviation assets

Aviation assets not covered under the Application Rules are **strongly encouraged** to voluntarily report cyber security incidents.

Cyber security incidents include:

- unauthorised access to computer data or a computer program;
- unauthorised modification of computer data or a computer program;
- unauthorised impairment or electronic communication to or from a computer; and
- unauthorised impairment of the availability, reliability, security or operation of a computer, computer data or a computer program.

Responsible entities are generally the aircraft operator, regulated air cargo agent, or airport operator.

Responsible entities must report:

- cyber security incidents having a **significant impact** within **12 hours** of becoming aware of the incident; and
- cyber security incidents having a **relevant impact** within **72 hours** of becoming aware of the incident.

Incidents can be reported via the [ACSC website](#) or the ACSC hotline: **1300 292 371**.

Hotline reports must be followed up by a written report via the website within **84 hours** for critical incidents and **48 hours** for other incidents.

A **significant impact** means your asset is used in connection with the provision of essential goods or services and the incident has materially disrupted the availability of those goods or services.

A **relevant impact** means that the availability, integrity or reliability of, or confidentiality of information about, your asset has been impacted in some way.

What is the data storage or processing services notification obligation?

Critical aviation assets (as defined in the [SOCI Act](#)) with **data storage or processing services** that are provided on a commercial basis and relate to **business critical data** need to notify the data storage or processing provider under [subsection 12F\(3\) of the SOCI Act](#).

Business critical data means:

- personal information that relates to at least 20,000 individuals;
- information relating to any research and development in relation to a critical infrastructure asset;
- information relating to any systems needed to operate a critical infrastructure asset;
- information needed to operate a critical infrastructure asset; or
- information relating to risk management and business continuity in relation to a critical infrastructure asset.

Are there other reporting requirements?

This does not impact reporting obligations that critical aviation assets and other aviation assets may have under other legislation. For example, Part 6 of the [Aviation Transport Security Act 2004](#) establishes reporting obligations in relation to *aviation security incidents* and there are notifiable data breach obligations under the [Privacy Act 1988](#).

What are 'systems of national significance'?

Assets that the Minister for Home Affairs declares to be a system of national significance (SoNS) have **Enhanced Cyber Security Obligations** under Part 2C of the [SOCI Act](#). If the Minister declares a critical aviation asset to be a SoNS, that critical aviation asset will be notified.

SoNS are the assets **most crucial to the nation**, by virtue of their interdependencies across sectors and potential for cascading consequences to other critical infrastructure assets and sectors if disrupted.

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.