Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

# Cyber Security Incident Reporting

The *Security of Critical Infrastructure Act 2018* (the SOCI Act) provides for mandatory cyber incident reporting for critical infrastructure assets. Critical infrastructure owners and operators are required to report a cyber security incident if they are captured by the critical infrastructure asset definitions as outlined below.

## What is a 'Cyber Security Incident'?

A cyber security incident is one or more acts, events or circumstances involving:

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

## What do I need to report?

**Reporting Critical Cyber Security Incidents**

If you become **aware** that a critical cyber security incident has occurred, or is occurring, AND the incident has had, or is having, a **significant impact** on the availability of your asset, you must notify the Australian Cyber Security Centre (ACSC) **within 12 hours** after you become **aware** of the incident. If you make the report verbally, you must make a written record through the ACSC's website **within 84 hours** of verbally notifying the ACSC.

A significant impact is one where both the critical infrastructure asset is used in connection with the provision of essential goods and services; and the incident has materially disrupted the availability of the essential goods or services delivered by a critical infrastructure asset or any of the circumstances specified in the rules exist in relation to the incident. For example, a critical cyber security incident might impact an electricity asset's operational technology, which impacts the generation, transmission, or distribution of electricity.

**Reporting other Cyber Security Incidents**

If you become **aware** that a cyber security incident has occurred, or is occurring, AND the incident has had, is having, or is likely to have, a 'relevant impact' on your asset you must notify the ACSC **within 72 hours** after you become **aware** of the incident. If you make the report verbally, you must make a written record through the ACSC's website within **48 hours** of verbally notifying the ACSC.

A relevant impact is an impact on the availability, integrity, reliability or confidentiality of your asset. For example, a cyber security incident might impact a bank's information technology (e.g. corporate network), might be impacted in a manner that could expose information about the asset, but not impact the provision of banking services.

## How do I make a report?

If there is a threat to life or risk of harm, call 000 immediately.

Urgent oral reports can be made to 1300Cyber1 (1300 292 371).

You can also report a cyber security incident on the ACSC's website (Report a cyber security incident | Cyber.gov.au). The ACSC has developed a tailored webform for submitting incident reports, which went live on 1 March 2022. Simply choose the link to report on behalf of a critical infrastructure organisation.

## When does the requirement commence?

The *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022* (the Application Rules) commenced on 08 April

# Cyber Security Incident Reporting

2022 (the commencement date). If your asset was a critical infrastructure asset specified in section 5 of the Application Rules on the commencement date, you are required to provide cyber incident reports but a grace period exists until **08 July 2022** to allow for transition.

This 3 month period before formal reporting obligations begins to assist asset owners and operators prepare business operations and procedures to comply with the cyber incident reporting requirement.

Prior to the commencement of the requirement to report cyber security incidents, the Department of Home Affairs strongly encourages all critical infrastructure asset owners to voluntarily report cyber security incidents to the ACSC.

## Which critical infrastructure sectors and asset classes are required to submit a report?

The critical infrastructure sectors and asset classes that are specified in section 5 of the Application Rules are required to submit a report, and these are:

- a critical broadcasting asset
- a critical domain name system
- a critical data storage or processing asset
- a critical banking asset
- a critical superannuation asset
- a critical insurance asset
- a critical financial market infrastructure asset
- a critical food and grocery asset
- a critical hospital
- a critical education asset
- a critical freight infrastructure asset
- a critical freight services asset
- a critical public transport asset
- a critical liquid fuel asset
- a critical energy market operator asset
- a critical port
- a critical electricity asset
- a critical gas asset
- a critical water asset, and
- a critical aviation asset that is 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.

Critical infrastructure sectors and assets not covered by these rules may have other reporting requirements under other legislation or regulation and are also encouraged to voluntarily report cyber security incidents.

## Which phase of malicious cyber activity might trigger the reporting requirement?

Whether you are **aware** that a cyber security incident has, or is happening is a matter of fact and relates to whether you or an employee of an asset has knowledge of that incident. For example, an employee may have observed unauthorised access to the responsible entity's computer system or a ransomware lock screen on the responsible entity's computer screen

Every cyber security incident is different and will impact critical infrastructure asses in unique ways.

Cyber security incidents typically involve several phases of malicious activity. An actor might conduct **reconnaissance** (e.g. scan network gateways for open ports), **deliver malicious software** (e.g. sending phishing emails), **exploit unauthorised access** to install malicious code (e.g. installing ransomware), and **undertake subsequent malicious activities** using that access (e.g. steal data or change how systems operate).

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

# Cyber Security Incident Reporting

If you detect a cyber security incident at or beyond the exploitation phase of malicious activity – irrespective of any prevention or mitigation action taken – you are required to submit a report. The exploitation phase represents the phase at which the availability, confidentiality and integrity of networks and network data has or could be impacted. This is also the phase where organisations will typically commence incident response processes.

If a cyber security incident is detected during the reconnaissance or delivery phases, you are strongly encouraged to voluntarily report this to the ACSC. This information could help to identify an emerging cyber campaign targeting Australia and better understand the cyber threat to Australia, critical infrastructure, and specific sectors.

As technical cyber security leads for the Australian Government, the ACSC is uniquely positioned to provide assistance and advice to victims of malicious cyber activity, including incident response services where appropriate.

## What information will I need to report?

The reporting process is designed to enable organisations to use a single report to notify the ACSC of an incident, seek technical advice or support from the ACSC to respond to the incident, and meet cyber security incident reporting requirements under the SOCI Act.

From a regulatory perspective, the form is designed to ensure that you can report either critical cyber security incidents having a significant impact or other cyber security incidents having a relevant impact on the asset.

To make a report, you will be asked to provide the following:

- point of contact information;
- organisation information (including Australian Business Number (ABN));
- 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.

## Will the report be provided to the Department of Home Affairs?

**Yes, but only with your organisation's consent**.

The ACSC webform will prompt you to provide consent to share the report with the Department of Home Affairs.

## Will the report be forwarded to other Commonwealth, state and/or territory regulators?

Not at this stage. The report will only be forwarded to the Department of Home Affairs as the critical infrastructure security regulator.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

# Cyber Security Incident Reporting

Critical infrastructure asset owners and operators may also be required to report the cyber security incidents and additional information to other regulators.

The Department of Home Affairs will engage with relevant Commonwealth, state, and territory departments and agencies to identify opportunities for facilitating the provision of incident reports to other regulators.

## How will the information be used?

The information will enhance the Australia Government's ability to develop strategies to identify and respond to national security risks for assets which, if disrupted, would significantly impact Australia.

The Department of Home Affairs will use your report for regulatory purposes under the SOCI Act. The information will also inform engagement with critical infrastructure asset owners and operators on cyber security risks.

The ACSC will also use your report to inform its understanding of the cyber threat to Australia.

## What will happen once I have reported?

You will receive a receipt of your report from the ACSC. This will include a unique Report Reference Number. It will also include information on whether you have consented to share your report with the Department of Home Affairs.

Depending on the nature of the incident, the ACSC may contact you to offer assistance or to obtain additional information about the incident for incident response and cyber threat information purposes.

Following an incident, the Department of Home Affairs may also contact you to obtain additional information about the incident for regulatory purposes.

## Can I access a copy of the report?

**Yes, but you will initially need to request a copy of the report from the ACSC at asd.assist@defence.gov.au.**

The webform will soon be updated to enable you to download a copy at the time you submit a report. The ACSC will not automatically send you a copy of your report for security reasons. This process will balance ACSC and Department of Home Affairs' cyber security and regulatory reporting requirements (respectively).

If an incident is ongoing, an organisation may not be able to access its information technology systems. Similarly, sophisticated malicious cyber actors may also be monitoring your organisation's communications channels (including email) to understand how you are responding to the incident to help them avoid further detection.

## Further information

For further information on cyber security incident reporting requirements, please contact enquiries@cisc.gov.au.