Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Cyber Security Incident Reporting

The *Security of Critical Infrastructure Act 2018* mandates cyber incident reporting for critical infrastructure assets. Critical Infrastructure owners and operators are required to report a cyber security incident if you are captured by the critical infrastructure asset definitions.

What is a Cyber Security Incident?

A cyber security incident is one or more acts, events or circumstances involving unauthorised access, modification or impairment of computer data, a computer program or a computer.

Whether you are aware of a cyber security incident is a matter of fact and relates to whether you or an employee of an asset has knowledge – for example, an employee observing, in real-time or a history of, unauthorised access to the responsible entity's computer system, or an employee observing a ransomware lock screen on the responsible entity's computer screen.

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.

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 those essential goods or services.

If you make the report verbally you must make a written record and provide the written record to **cyber.gov.au/report** within **84 hours** of verbally notifying the ACSC.

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 the availability of your asset you must notify the ACSC within **72 hours** after you become aware of the incident.

A **relevant impact** is an impact on the availability, integrity, reliability or confidentiality of your asset.

If you make the report verbally you must make a written record and provide the written record to **cyber.gov.au/report** within **48 hours** of verbally notifying the ACSC.

How to make a Report

If there is a **threat to life or risk of harm, call 000 immediately**. You can report a cyber security incident on the ACSC's website (**cyber.gov.au/report**). Urgent oral reports can also be made to 1300Cyber1 (**1300 292 371**).

What information should the report include?

All materials are available at cyber.gov.au/report. To make a report, you will need the following information: your contact details in information on your organisation (including Australian Business Number (ABN)); the nature of the incident being reported and when it was first identified; how the incident was discovered; and whether the incident was reported elsewhere.

Why do I need to report?

By reporting, you will be helping to stop other people from falling victim to the same issue. Your report will also assist the ACSC and law enforcement agencies to disrupt cyber-crime operations and make Australia the safest place to connect online.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Cyber Security Incident Reporting

What will happen once I have reported?

You will receive a receipt of your report for the ACSC that has a unique Report Reference Number. All reports made to the ACSC will help to identify emerging cyber threats that may be affecting you or others across the different critical infrastructure sectors. The ACSC may contact you to offer assistance or to obtain additional information.