Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE SECURITY CENTRE

Notification of Cyber Security Incidents

Security of Critical Infrastructure Act 2018

Contact us

Enquiries regarding the licence and any use of this document are welcome to **CI.strategy.guidance@homeaffairs.gov.au** or:

Critical Infrastructure Security Policy,
Department of Home Affairs
PO Box 25, BELCONNEN, ACT 2616

Contents

Preface

This guidance has been prepared to assist specified critical infrastructure entities to comply with their 'Notification of cyber security obligations' as per **Part 2B** of the ***Security of Critical Infrastructure Act 2018*** **(SOCI Act**). This obligation is commonly referred to as Mandatory Cyber Incident Reporting (MCIR).

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.

What is the notification of cyber security incidents obligation?

Notification of cyber security incident (NCSI) reporting is the obligation to report 'critical' or 'other' cyber security incidents that have an impact on critical infrastructure assets to the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), which receives and manages cyber security reports.

If an incident has occurred, or is occurring AND the incident has had or is having a '**significant impact'** (whether directly or indirectly) on the availability of your asset, then it is a ***critical*** cyber security incident.

Critical cyber security incidents must be reported to the ASD's ACSC within **12 hours** of becoming aware of the incident. If you make the report verbally, you must also make a written record (through cyber.gov.au) within 84 hours of verbally notifying the ASD's ACSC.

If an incident has occurred, is occuring, or is imminent AND the incident has had, is having, or is likely to have a '**relevant impact'** (whether directly or indirectly), then it is an ***other*** cyber security incident.

Other cyber security incidents must be reported to the ASD's ACSC within **72 hours** of becoming aware of the incident. If you make the report verbally, you must also make a written record (through cyber.gov.au) within 48 hours of verbally notifying the ASD's ACSC.

How do I make a report?

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

To make a written report go to cyber.gov.au/report

To make a verbal report call 1300 CYBER1 (1300 292 371)

What is a cyber security incident under the SOCI Act?

A cyber security incident is defined in **section 12M** of the SOCI Act as being one or more acts, events or circumstances involving:

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

Once you have determined that a cyber security incident has occurred, is occurring, or is imminent, you will need to assess its impact or potential impact and decide whether it is ***relevant*** or ***significant***. This determines whether the incident is classified as ***critical*** or ***other*** and sets the reporting timeframe.

The Department considers it is best practice for responsible entities to also notify of any cyber security incident where third-party providers advise responsible entities that the responsible entities' business critical data has been compromised.

What is 'unauthorised'?

For the incident to be unauthorised, it must have occurred without the consent of the responsible entity or without lawful justification. **Section 12N** of the SOCI Act, outlines what is considered to be unauthorised.

This may be when an employee does something that is outside their job role or without the required approval, for example, an employee modifying computer data when they are only entitled to view the data. It may also be when someone with no authority, for example someone who does not work in a company, undertakes an action to access computer data of that company.

The person responsible for the unauthorised action does not need to be identified for the action to be considered unauthorised. For example, if a computer program was impaired, and it is not clear who impaired it, but the action would not ordinarily be within anyone's job role, the action is still unauthorised despite not knowing who caused the action.

For an action to be unauthorised it does not need to be intentional. An accident that results in unauthorised access, modification, or impairment is still considered a cyber security incident.

A person is entitled to cause access, modification or impairment if they do so under or in accordance with certain warrants, authorisations, requests or notices listed in **section 12N(3)(b)**. For example, if an employee performs a task that is outside their job role, but in accordance with a police warrant, the action would not be considered unauthorised.

What is unauthorised 'access to computer data or a computer program'?

Unauthorised access to computer data or a computer program is defined in **section 5** of the SOCI Act. It is the action of viewing, copying or moving data without the permission to do so. This could include unauthorised:

- access to a computer program, for example, an employee viewing a program that designed a schematic of a gas pipeline without permission to do so.

- display of data by a computer or any other output of the data from the computer, for example, the unauthorised viewing of schematics of a gas pipeline
- copying or moving of the data to another location in the computer, to another computer, or to a data storage device. For example, the employee emailing the schematics of a gas pipeline to a personal computer.

What is unauthorised 'impairment of electronic communication to or from a computer'

Impairment of electronic communication to or from a computer is defined in **section 5** of the SOCI Act. It includes preventing communication, and the impairment of communication, on an electronic link or network used by the computer.

It does not include the interception of communication unless that interception results in the prevention or impairment of the communication.

This could include:

- Denial of service attack that blocks access to a website
- A virus that does not allow legitimate emails to be sent.

What is unauthorised 'modification'?

Modification is defined in **section 5** of the SOCI Act and means the alteration, removal or addition to computer data or a computer program.

An example of this could be a person without authorisation installing a new program onto a computer that tracks the keystrokes, or a person without authorisation removing or altering the virus protection software.

Incidents that generally do not need to be reported

While organisations are encouraged to report cyber security incidents, potential incidents and vulnerabilities to ASD's ACSC, not all incidents are covered under the NCSI reporting obligation in the SOCI Act. Incidents that are unlikely to be covered by the reporting obligation include:

- **Scam calls and emails**: these do not need to be reported unless they lead to infiltration of computer data or programs, resulting in unauthorised access modification or impairments to computer systems or information.
- **Social engineering and suspicious contacts**: these do not need to be reported unless they lead to a cyber security incident such as infiltration of computer data or programs, e.g. through obtaining employee credentials, giving unauthorised access to your organisation's computer data and/or programs.
- **Incidents relating to data storage systems** in which the incident did not impact the storing of business critical data of the critical infrastructure asset.

You should take steps to protect your people, information and assets against threats like these.

Remember, while these might not require NCSI reporting, entities can still voluntarily report all cyber security incidents and vulnerabilities to the ASD's ACSC, who can offer incident response advice and assistance. You are able to indicate that you are voluntarily reporting in the free text field. Reporting helps ASD and the Department of Home Affairs protect and prevent harm to others who might be vulnerable.

Asset classes with notification of cyber security incidents obligation

Sector	Asset class	Notification of cyber security incident obligation
Energy	Critical Electricity Assets[1]	✓
	Critical Gas Assets	✓
	Critical Energy Market Operator Assets	✓
	Critical Liquid Fuel Assets	✓
Communications	Critical Telecommunications Assets[2]	✓
	Critical Broadcasting Assets	✓
	Critical Domain Name System Assets	✓
Data Storage & Processing	Critical Data Storage or Processing Assets	✓
Financial Services & Markets	Critical Banking Assets	✓
	Critical Superannuation Assets	✓
	Critical Insurance Assets	✓
	Critical Financial Market Infrastructure Assets	✓
Water & Sewerage	Critical Water Assets	✓
Healthcare & Medical	Designated Hospital	✓
	Critical Hospital Assets	✓
Higher Education & Research	Critical Education Assets	✓
Food & Grocery	Critical Food and Grocery Assets	✓
Transport	Critical Ports[3]	✓
	Critical Freight Infrastructure Assets	✓
	Critical Freight Services Assets	✓
	Critical Public Transport Assets	✓
	Critical Aviation Assets[4, 5]	✓
Space Technology	No Assets currently defined	
Defence Industry	Critical Defence Assets	

[1] Some sugar mills are excluded, see section 5 of the Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022

[2] Only applies to telecommunications assets that are owned and operated by a carrier **or** a relevant carriage service provider asset.

[3] Assets which are critical maritime assets on or after the commencement of Part 1 of Schedule 3 to the *Transport Security Amendment (Critical Infrastructure) Act 2022* are excluded.

[4] As per section 5 of the *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022* – Only applies to aviation assets that are any of the following:

A. A designated airport;

B. An asset used to perform an Australian prescribed air service operating screened air services that depart from a designated airport;

C. A cargo terminal that:

i. Is owned or operated by a regulated air cargo agent that is also a cargo terminal operator; and

ii. Is located at a designated airport

[5] Assets which are critical aviation assets on or after the commencement of Part 1 of Schedule 3 to the *Transport Security Amendment (Critical Infrastructure) Act 2022* are excluded.

Identifying a reportable cyber security incident

For a cyber security incident to be reportable (under Part 2B of the SOCI Act) it must meet the definition of a cyber security incident in **section 12M** of the SOCI Act, and it must have either:

- a significant impact on the availability of the asset
- a relevant impact on the asset.

The type of impact informs the reporting timeframes, as such it is important to understand what constitutes a significant or relevant impact. These definitions should be included in your cyber security incidents response plan to assist you in being compliant with your reporting obligations.

Significant impact

A significant impact is defined in **section 30BEA** of the SOCI Act. A cyber security incident has a significant impact on the availability of an asset 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.

The incident does not have to have a direct significant impact on the asset for it to be reportable. For example, if a Managed Service Provider's product that is integral to the provision of your service goes down, and as a result your asset is not able to function, the incident must be reported.

Indicators of significant impact may include:

- You lose control of your operating technology
- Your asset is unable to function as intended and you are unable to deliver services
- You shut down essential services to contain the impacts of the incident.

When assessing whether the impact is significant, you should consider what the essential goods or services are that your asset is providing. Doing this will assist you to determine whether the availability of those essential goods or services have been impacted.

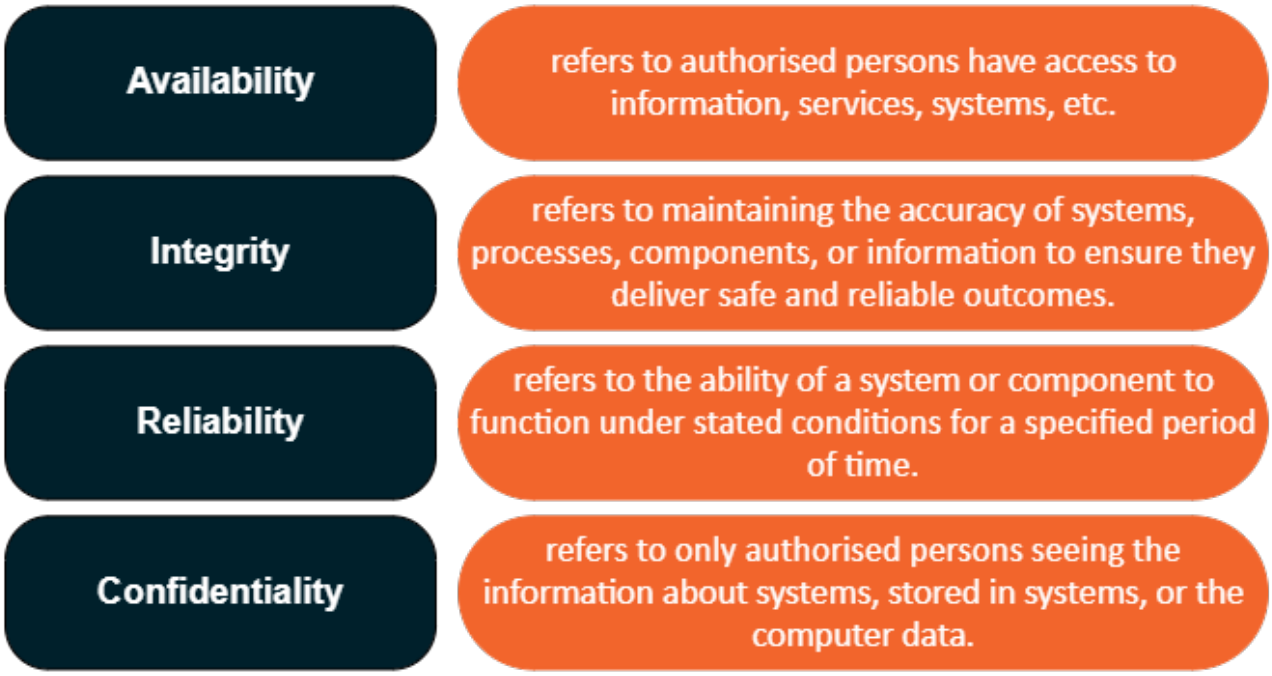
If it is determined that the cyber incident is having a **significant impact** on the availability of the asset, then the incident is considered to be a **critical cyber security incident** (**section 30BC**).

For example, a critical cyber security incident might impact an electricity asset's operational technology, which impacts the generation, transmission, or distribution of electricity.

See Attachment A for examples.

Relevant impact

A relevant impact is defined in **subsection 8G(2)** of the SOCI Act. It is an impact on the availability, integrity, reliability or confidentiality of a critical infrastructure asset. The impact can be directly or indirectly related to the incident.



Indicators of relevant impact may include:

- your corporate systems are impacted which, for example, inhibits your internal communications systems or customer records
- however, your asset is still able to operate as it is designed to and deliver core functions.

If it is determined that the cyber incident is having a **relevant impact** to the availability to the asset, then the incident is an **other cyber security incident** (**section 30BD**).

For example, a cyber security incident might impact a bank's information technology (e.g. corporate network). The incident may have exposed customer information or information relating to the asset, however it did not impact the provision of banking services. This would be a relevant impact.

See Attachment A for examples.

When do you need to report?

Critical cyber security incidents

As per **section 30BC** of the SOCI Act, you must report a **critical cyber security incident** as soon as practicable after you become aware that:

- the incident has occurred or is occurring **and**
- it has had, or is having, a **significant** impact on the availability of the asset.

If the incident is a **critical cyber security incident**, you are obligated to report this within **12 hours** of becoming aware of the incident. This can be done orally or in writing. If you elect to provide the report orally, you must also provide a written copy of the report within **84 hours** of providing the oral report.

If you have reported an 'other cyber security incident' and subsequently the impact becomes significant, then you must submit a second report within **12 hours** of becoming aware that it is having a significant impact and, if the second report is an oral report, a written report within **84 hours**.

Failure to provide a report to the ASD's ACSC, in the approved form, may result in a civil penalty under **section 30BC** of the SOCI Act.

Other cyber security incidents

As per **section 30BD** of the SOCI Act, you must report an **'other cyber security incident'** as soon as practicable after you have become aware that:

- that the incident has occurred, is occurring, or is imminent **and**
- it has had, is having, or is likely to have, a **relevant impact** on the asset.

If the incident is an **'other cyber security incident'**, you are obligated to report this within **72 hours** of becoming aware of the incident. This can be done orally or in writing. If you elect to provide the report orally, you must also provide a written copy of the report with **48 hours** of providing the oral report.

Failure to provide a report to the ASD's ACSC, in the approved form, may result in a civil penalty under **section 30BD** of the SOCI Act

When do you 'become aware' an incident is occurring?

'Becoming aware' is a matter of fact and relates to whether the responsible entity of an asset has knowledge of that incident. A responsible entity is considered to have become aware of an incident when a person within the entity who has **responsibility for, or an ability to identify a cyber security incident** knows or should have known that a cyber security incident has occurred.

A responsible entity is not considered to become aware merely because an automated system has detected an incident. The entity becomes aware when there has been confirmation that the incident has taken place, or the entity should have become aware if they were following their monitoring and escalation processes.

For example:

- A responsible entity has a 24/7 incident detection capability, and an expectation that all flags would be checked as soon as they appear. The entity is considered to have become aware at the time of the system raising a flag.
- A responsible entity does not have a 24/7 incident detection and response capability. Their IT system flags an irregular occurrence at 4 am. The system is not reviewed until standard business hours (9 am). The entity is considered to have become aware at 9 am, when the system is scheduled to be checked, and the entity ought to have become aware.
- A HR employee observes a ransomware lock screen on a responsible entity's computer system at 10am. It is reasonable to expect that an employee without cyber security training could identify that a cyber security incident is occurring. The entity is considered to have become aware at 10am, when the employee sighted the incident.

In contrast, an employee without cyber security training who experiences a more discreet incident may not be considered to have the ability to identify that the incident was a cyber security incident. For example, an HR employee receives what they believe is a legitimate request to update their computer. At 10 am they undertake the update and afterwards their computer is running slower than usual. At 11 am they log a ticket with the IT help desk to resolve the issue. The HR employee does not realise that this can be a sign of a cyber attack. The IT help desk reviews the ticket within two

hours of receiving it and discovers malware has been installed on the employee's computer. The entity became aware when the IT help desk reviewed the ticket. This means at 1pm, when the ticket was reviewed, the responsible entity became aware of the incident

Considering the above example, the responsible entity's standard operating procedure outlines that the IT help desk must triage tickets and prioritise potential incidents within 2 hours of receiving them. The IT help desk fails to triage the ticket, and they don't review the ticket until the following day. The responsible entity ought to have known about the incident by 1 pm, and as such they are considered to have become aware at 1 pm.

Stages of an incident

Every cyber security incident is different and will impact critical infrastructure assets 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 emails that may include malicious attachments or directed the user to download a malicious file, otherwise known as phishing)
- exploit unauthorised access to install malicious code (e.g. installing ransomware)
- undertake subsequent malicious activities using that access (e.g. steal data or change how systems operate).

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.

Pre-positioning is the process in which computer code is installed on a network or system to allow for future hostile cyber activity. This means that pre-positioning falls into the 'exploitation' phase of malicious activity and is likely to meet the criteria of being an 'other' cyber security incident.

If a cyber security incident is detected during the reconnaissance or delivery phases, you are strongly encouraged to voluntarily report this to ASD's ACSC. This information could help better understand the cyber threats to Australia, critical infrastructure, and specific sectors. As technical cyber security leads for the Australian Government, ASD is uniquely positioned to provide assistance and advice to targets of malicious cyber activity, including incident response services where appropriate.

If you submit a voluntary report during the reconnaissance or delivery phase, you are still required to submit a report if it progresses to exploitation or unauthorised access phases. This is because the earlier report is not considered a notification of cyber security incident report. When the incident progresses to having a relevant impact, then a report must be made within 72 hours.

What kind of information must be provided in the report?

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

We acknowledge that you may not be able to provide all of the relevant information at the time of making a report. The impact of the incident may change, and the extent of the impact may not be

clear at the initial reporting phase. The CISC encourages entities to provide additional reports should further information become available.

If the impact of the incident changes from a *relevant impact on the asset* to a *significant impact on the availability of the asset* then you are obligated to provide another report within 12 hours of becoming aware that the impact has had a significant impact on the availability of the asset.

What happens after you report?

You will receive a receipt acknowledging your report from the ASD's 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. Depending on the nature of the incident, the ASD's ACSC may contact you to offer assistance or to obtain additional information about the incident for response and cyber threat information purposes.

For security reasons, you will not automatically be provided a copy of your report. You can request a copy of the report at asd.assist@defence.gov.au.

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

What happens if you report late or do not report at all?

You should report an incident as soon as practicable after becoming aware of its occurrence and impact.

You should not delay making a report to obtain more information. We recommend making a report early and providing as much information as possible. You can then follow up with another report providing additional details. A detailed report allows us to assist you and other impacted businesses and organisations and ensures a quicker recovery from attacks, but it is more important to ensure a report is made promptly than to include every possible detail and delay the report.

If you do not report an incident, or you do not include sufficient information when that information is known to you, we cannot help you and other businesses and organisations across Australia to protect yourselves or recover as quickly from attacks. Unreported breaches and attacks can ultimately hurt our community and economy.

If you have missed the timeframe for reporting, you should still make a report. Late reports will be considered less egregious and are less likely to result in punitive action than not reporting at all.

Failure to make a report to the ASD's ACSC, in the approved form and within the approved timeframe, may result in being subject to a civil penalty under **sections 30BC** or **30BD** of the SOCI Act.

The CISC will seek to work in partnership with industry to ensure regulated entities understand and manage their own risk, encouraging voluntary compliance.

How is the information in a report used?

The information provided in a report will enhance the Australian 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 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.

ASD's ACSC will use your report to inform its understanding of the cyber threat to Australia and, if required, to assist you in recovering from the cyber security incident.

Reporting cyber security incidents is important because it helps build a clear picture of emerging threats and risks across Australia. This information enables the Australian Government to collaborate with industry and improve awareness of cyber attacks that can significantly disrupt critical services and businesses.

The reports also allow experts to support organisations during serious incidents by providing timely advice. Ultimately, this helps critical infrastructure operators maintain the essential services that our community and economy depend on.

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

The webform will prompt you to provide consent to share the report with the Department. The report will only be forwarded to the Department, as the critical infrastructure security regulator. Without your consent, ASD's ACSC is unable to share your report to the Department.

The National Office of Cyber Security (NOCS) will also receive a copy of your report if you consent to sharing it with the Department. If NOCS becomes aware of the incident through open source information they may still reach out to offer their assistance.

The information provided to the Department allows us to uplift security, informs policy advice, and improves guidance products designed to help support industry in the uplift of their resilience. Sharing the report with the Department will also ensure you are not approached for being non-compliant with your reporting obligation, when a report has in fact been made. We strongly encourage entities to share the reports with the Department.

Critical infrastructure asset owners and operators may also be required to report the cyber security incident and additional information to other regulators. The Department will not on-share the report for the purpose of meeting other regulatory obligations.

National Office of Cyber Security

The National Office of Cyber Security (NOCS) supports the National Cyber Security Coordinator (the Coordinator) to deliver their functions under the Australian Government Crisis Management Framework (AGCMF) and Australian Cyber Response Plan (AUSCYBERPLAN). The Coordinator manages responses to cyber security incidents of national significance or interest. They are accountable to the Minister for Cyber Security.

The NOCS is the central touchpoint for affected organisations. The NOCS works collaboratively to help consequence management efforts of an incident across Australian, state, and territory government departments and agencies.

Consequence management relates to the second and subsequent order effects from cyber security incidents. The NOCS helps government and industry work together to identify and mitigate the secondary harms that may result from a cyber security incident. In the most severe instances, this could include 'real world' impacts. This may require the activation of emergency management arrangements, such as the National Coordination Mechanism.

The NOCS may contact you in relation to your report to help coordinate the response and engagement across government. Information you provide to the NOCS may be subject to limited use protections (contact nocs.response@homeaffairs.gov.au for further information).

ASD's ACSC remains the Australian Government's technical cyber security authority.

Protected information and limited use

Protected information

The SOCI Act limits the use and disclosure of 'protected information' as defined within section 5A of the SOCI Act. Protected information includes information obtained in the course of exercising powers or performing functions or duties under the SOCI Act; this includes the information you provide as part of a notification of cyber security incident.

It is an offence to use or disclose protected information unless for an authorised purpose. Unauthorised use or disclosure of protected information is punishable by 2 years imprisonment or 120 penalty units, or both.

Importantly, the phrase "protected information" under the SOCI Act is different from the PROTECTED security classification under the Australian Government's Protective Security Policy Framework (PSPF).

Limited use

Division 1A of the *Intelligence Services Act 2001* and Division 3 of the *Cyber Security Act 2024* provide schemes for the limited disclosure of information that organisations provide to ASD and/or the National Cyber Security Coordinator about cybersecurity incidents and potential incidents, including vulnerabilities.

This scheme does not apply to information about a cyber security incident provided to the Commonwealth to comply with your obligations under Part 2B of the SOCI Act.

It is important to note that information reported to ASD under the notification of cyber security incidents obligation is not covered by limited use provisions.

A step-by-step guide: Reporting a Cyber Security Incident

Before you begin completing the report

The form is a single page and is divided into 3 different sections. If you begin completing the form and decide to finish it at a later time, you will have to re-complete the entire form **as it will not save a draft** for you.

Do not complete this form on any network you believe has been compromised. You should use a separate system and contact details to submit the form. This is because 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.

Access the form at Report a cyber security incident | Cyber.gov.au/report

Reporting a Cyber Security Incident

Reason for reporting (please select all that apply)?

- ☐ To inform the Australian Cyber Security Centre (ACSC)
- ☐ To request assistance or advice from the Australian Cyber Security Centre (ACSC)

Tips to respond

Select the appropriate reasons for reporting the incident. If the incident is ongoing, it is recommended that you also select the second option to receive assistance or advice from the ASD's ACSC.

Contact details

- ☐ First name
- ☐ Last name
- ☐ Email address
- ☐ Verify email address
- ☐ Contact number

Tips to respond

When inputting contact details, consider that this person will be approached should you require assistance, or should more information be required. It is important you provide someone who is

easily contactable, and with appropriate authority to provide what is required to the ASD's ACSC or the Regulator. It is preferred that you provide an individual as your contact person, and provide the individual's contact details, so that the person can be reached, as opposed to a group inbox or generic phone line.

How we use the information

There are two primary ways the Department uses information provided under the notification of cyber security incidents obligation.

The National Office of Cyber Security (NOCS) provides incident consequence management assistance to entities that have experienced a cyber security incident. The NOCS will contact the person listed in the form to offer this assistance. It is important that you provide an individual email and contact number rather than a group inbox or generic contact line as this allows them to reach the correct person swiftly and provide timely assistance to you in managing the impact of the incident.

The Critical Infrastructure Security Centre (CISC) assesses the reports provided and considers whether the SOCI obligation has been met. In the event of a non-compliance with reporting obligations, the CISC is likely to reach out to the contact person provided in the report.

Organisation details

- Organisation name
- ABN
- State/Territory
- Postcode
- Website address

Tips to respond

These details should be of the affected entity.

Is your organisation part of a critical infrastructure sector?

- Yes
- No

Tips to respond

If your organisation is a part of a critical infrastructure sector, select yes. Two more questions will appear beneath this asking to identify your critical infrastructure sector and asking for your consent to send the report to the Department.

Select your critical infrastructure sector(s)?

- ☐ Telecommunications
- ☐ Other communications sector
- ☐ Financial services and markets
- ☐ Data storage or processing
- ☐ Defence industry
- ☐ Higher education and research
- ☐ Energy
- ☐ Food and grocery
- ☐ Health care and medical
- ☐ Space technology
- ☐ Transport, including aviation and maritime assets
- ☐ Water and sewerage
- ☐ Not listed

Do you consent for this cyber incident report to be provided to the Department of Home Affairs to meet mandatory regulatory reporting requirements?

Tips to respond

If the cyber security incident meets the threshold to become a NCSI report, you should select "yes". If you are unsure, select "yes".

If you do not select 'yes' and the report is a NCSI report, you may be approached to confirm you have provided a report to ensure you are compliant with your reporting obligations.

How we use the information

Sharing the report with the Department allows us to better understand the cyber incident impacts on critical infrastructure. This allows us to uplift security, informs policy advice, and improves guidance products designed to help support industry in the uplift of their resilience. Sharing the report with the Department will also ensure you are not approached for being non-compliant with your reporting obligation, when a report has in fact been made. We strongly encourage entities to share the reports with the Department.

NOCS will also receive a copy of your report if you consent to sharing it with the Department.

Date and time incident was identified

Tips to respond

Provide the date and time as accurately as possible. The time is provided in AM/PM format. Provide the date and time in the time zone that your organisation is based in.

An entity becomes aware of an incident when a person within the responsible entity who has responsibility for, or the ability to assess, cyber security risks knows or should have known that a cyber security incident has occurred and meets the reporting threshold under the SOCI Act. You can read more about this on page 11 of this guidance.

Is the incident ongoing?

Tips to respond

If the incident is continuing to affect the entity select yes. Otherwise, if the incident has been finalised, select no.

*NCSI reporting does not require ongoing reporting. However, if the incident impact becomes **significant**, where it was previously a **relevant** impact, then you are required to submit another report within 12 hours of becoming aware that the impact was significant.*

How we use this information

This information allows the Government to understand whether you are likely to need assistance managing the incident, or whether you have a full understanding of the nature or impact of the incident at this stage.

The NOCS assists entities in consequence management following an incident, and if necessary while the incident is occurring. It is important that they are aware of whether the incident is ongoing so they can ensure that when they seek to assist they are not interfering with or drawing resources away from the containment and response during an ongoing incident.

Which of the following are being impacted?

- ☐ Information technology systems
- ☐ Operational technology systems
- ☐ Customer data

Tips to respond

Select the appropriate box(es) that apply to the cyber security incident.

Information technology systems:

The hardware and software that make data available to, from or within an organisation. Examples include email, websites, file storage, VPN, CRM.

Operational technology systems:

The systems used to monitor and/or control physical devices, processes, and/or events. Examples include SCADA, PLCs, IoT, sensors, machinery, and assembly lines.

Customer data

Impacted entities should consider whether compromised systems contain personal or sensitive information, including scans or details of passports, driver's licences, tax file numbers, superannuation, tax file, Centrelink or medical information.

Was the incident identified by your organisation, or were you notified by a third party?

- ☐ Own organisation

- Third party

Please select the type of incident from the following

- Denial of service (DOS)
- Scanning and reconnaissance
- Unauthorised access to network or device
- Data exposure, theft or leak
- Malicious code/malware
- Ransomware
- Phishing/spear-phishing
- Other (please specify)

Tips to respond

Select the box(es) which best describe the cyber security incident that is impacting your asset. If you select "Other" a text box will appear beneath so that you can specify the incident further.

Denial of service (DOS):
Where systems are rendered unavailable due to an actor overloading or flooding the service with requests.

Scanning and reconnaissance:
Where networks have been queried, usually to identify potential vulnerabilities, or unsecured access vectors, for unauthorised access.

Malicious code/malware:
Involving software or scripts that are designed to damage files or systems, disrupt or deny access to files or systems, or to gain unauthorised access to files or systems.

Ransomware:
A type of malicious software, designed to deny access to files or systems until demands by an actor are met.

Phishing/spear-phishing:
Where fraudulent emails (purporting to be from a reputable source) are sent or received in order to gain unauthorised access to information.

How we use this information

This information allows the Department and the NOCS to gain an understanding of whether the incident is likely to be impacting other entities, the type of impact that may be experienced, and whether it is likely to be a campaign of cyber attacks, or a singular incident.

Please describe the incident including how it occurred and the observed activity (such as the extent of the incident, any data loss/modifications and the impact to your business operations)

Tips to respond

Describe the incident in as much detail as possible (noting the 1000 character limit) regarding:

- *how it occurred*
- *extent of the incident*
- *any data loss/modifications*
- *impact to business operations and delivery of service*
- *which systems have been taken offline, if any?*
- *initial estimate of impact including duration of outage*
- *the critical infrastructure asset that was affected*
- *any other information that may be relevant*

In the event that data has been exposed, it would be beneficial to include information around the type of data that has been exposed and the potential cascading impact. If the data exposed is owned by the Government, or if the exploited system or network is connected to Government systems, you should also consider providing this in your description.

When describing the extent of the incident, please detail whether the impact is likely to be isolated to one State or Territory, or whether there are, or could be, national consequences.

Consider whether other assets may be impacted by the incident, and whether there are any impacts on Government entities, at both Commonwealth and State or Territory levels.

How we use this information

This helps inform our response to the incident. The information you provide here will indicate to the NOCS whether you require assistance for consequence management, whether the impact will cascade beyond your entity, and how time sensitive the response will need to be.

It also allows the CISC to assess whether the incident meets the requirements to be considered a NCSI report.

Please provide any further details the ACSC may need to understand the effect of this incident. This may include detail on how you are responding to the incident.

Tips to respond

Describe the effect that the incident is having to your organisation/asset (noting the 1000 character limit) and any details about your response to the incident. Include details about:

- *can you still provide essential goods and services?*
- *whether the incident has been reported elsewhere*
- *any steps that have been taken to mitigate/prevent impact*
- *any other information that may be relevant*

If you have engaged with other State or Federal Government entities you can include this information here.

How we use this information

Providing information here about the steps you have already taken, the impact on your provision of services, and whether it has been reported elsewhere informs the Government response to the incident. If you have reported it to other agencies the Department is able to liaise with them and provide a coordinated response. Information around impact and mitigation steps already taken allow the Department to understand the response that has already been undertaken, and whether additional steps will need to be taken.

Form complete

You will only receive further communication from the CISC if we require more information.

If you would like further assistance or information, contact nocs.response@homeaffairs.gov.au

Attachment A: Examples of critical and other cyber security incidents

Critical Incident Examples

Critical Incident 1 – IT incident	
Circumstances	• An employee of a critical infrastructure entity has noticed the cursor moving on its own on one of the key corporate systems. The employee tries to take control of the computer, but they cannot. • Shortly afterwards, the corporate system becomes unavailable, which is directly impeding the ability of the asset to provide essential services, creating a large impact on customers.
Actions	• This would be considered a critical cyber security incident as it has resulted in material disruption to essential goods and services. • This must be reported to the ASD's ACSC within 12 hours of the employee noticing the corporate system was unavailable, i.e. when the incident was recognised as having a significant impact.
Critical Incident 2 – OT operating unpredictably	
Circumstances	• A freight rail operator identifies that signalling controllers and interlocking systems are responding unpredictably. Initial checks of the operational technology (OT) logs show unauthorised configuration changes pushed to multiple control locations via a remote access session. • As a safety measure, the operator halts all freight movements across major corridors. This immediately prevents the transport of liquid fuels, disrupting some critical infrastructure entities supply chains.
Actions	• This would be considered a critical cyber security incident because it materially disrupts the availability of essential services provided by a critical freight service asset. • This must be reported to the ASD's ACSC within 12 hours of the operator noticing essential services were unavailable, i.e. when the incident was recognised as having a significant impact.
Critical Incident 3 – Unexpected change in OT	
Circumstances	• A water treatment plant notices unexpected changes in chlorine dosing settings and pump operations on its control systems. Operators see unreliable readings and lose consistent control over several process units. • To protect public safety, the utility halts treatment and isolates distribution from the affected plant. This results in service interruptions to multiple suburbs and triggers precautionary boil-water advisories, constituting a material disruption to the availability of potable water.
Actions	• This would be considered a critical cyber security incident because it materially disrupts the availability of essential goods and services delivered by a critical water asset

	• This must be reported to the ASD's ACSC within 12 hours of the operator halting treatment, i.e. when the incident was recognised as having a significant impact.
Critical Incident 4 – Malicious actor pushing faulty configurations	
Circumstances	• A telecommunications company detects that someone has pushed bad configuration changes to core network routers (the devices that direct internet traffic). • This makes the network unstable and cause a widespread loss of mobile calls, text messages, and internet across several regions. • Customers, including emergency services, experience a major outage.
Actions	• This would be considered a critical cyber security incident for the critical telecommunications asset because it materially disrupts the availability of essential services (communications) provided by a critical infrastructure asset. • This must be reported to the ASD's ACSC within 12 hours of the operator noticing that there was a widespread outage, i.e. when the incident was recognised as having a significant impact. • In this example, this disruption may also have a significant or relevant impact for other critical infrastructure. Critical infrastructure entities affected must also report, based on the impact to their critical asset. • You should consider your obligations under Part 2D of the SOCI Act. You can read more about specific telecommunications obligations in the **Telecommunications Guidance**.
Critical Incident 5 – Stolen credential	
Circumstances	• An attacker uses stolen credentials to change a fuel terminal's control system and tank level settings. Safety checks are turned off, level readings are wrong, and the dispatch screens freeze. • To keep people safe and prevent spills, the operator stops loading trucks and pauses pipeline transfers. This means tankers can't load petrol, diesel, or jet fuel, and service stations, businesses, and airports don't get deliveries.
Actions	• This would be considered a critical cyber security incident because it materially disrupts the availability of the critical liquid fuel asset. • This must be reported to the ASD's ACSC within 12 hours of the operator halting services, i.e. when the incident was recognised as having a significant impact
Critical Incident 6 – Unauthorised changes to systems	
Circumstances	• A bank detects unauthorised changes made to systems that approve card transactions and route payments. As a result some ATMs stop processing withdrawals, EFTPOS terminals are unable to process payments, and many online card transactions fail. • The outage means customers can't withdraw cash or pay for goods and services, creating a material disruption to the availability of essential financial services.
Actions	• This is a critical cyber security incident because it causes the critical banking asset (card payments and ATM withdrawals) to be unavailable.

	• This must be reported to the ASD's ACSC within 12 hours of the operator noticing that payment systems have become unavailable, i.e. when the incident was recognised as having a significant impact. • In this example, this disruption may also have a significant or relevant impact for other critical infrastructure. Critical infrastructure entities affected must also report, based on the impact to their critical asset.
Critical Incident 7 – Abnormal commands on network	
Circumstances	• A electricity distributor detects abnormal commands on its control network. Field crews report substations tripping unexpectedly, causing widespread feeder outages across multiple towns. The control centre loses reliable command and visibility of remote devices. • The result is a material disruption to the availability of electricity, with customers unable to access power and downstream essential services.
Actions	• This would be considered a critical cyber security incident because it materially disrupts the availability of essential services delivered by a critical infrastructure asset. • This must be reported to the ASD's ACSC within 12 hours of the operator noticing that there are widespread outages, i.e. when the incident was recognised as having a significant impact.
Critical Incident 8 – Non-malicious incident	
Circumstances	• A gas pipeline operator relies on security software on computers in the control room and on field laptops. A scheduled update is conducted, however, the update is faulty and causes modifications to the software that were not authorised. Many computers then crash and won't boot. Operators can't reliably see or control the gas equipment. • To keep the network safe, the operator shuts down compressors and closes valves in affected areas. This cuts gas supply to industrial customers and electricity generators, causing a major disruption.
Actions	• This would be considered a critical cyber security incident as it involves an unauthorised modification and has resulted in a disruption to a critical gas asset. • This must be reported to the ASD's ACSC within 12 hours of the operator noticing they were unable to control the gas equipment, i.e. when the incident was recognised as having a significant impact.

Other Incident Examples

Other Incident #1 – Ransomware	
Circumstances	• An energy market operator goes to open an internal planning document relating to their asset and finds that it, along with thousands of related files, have been encrypted and they cannot access them. The internal IT department identifies that the entity's computer systems have been infected with malware. • The entity is contacted by cybercriminals who demand a ransom payment, otherwise they will leak the entity's non-public policies, plans and procedures to the dark web. • Whilst plans and procedures about the asset have been accessed, there is no impact to the entity's delivery of services, which continue functioning as normal.
Actions	• This would be considered an "other" type of reportable incident as it has had a relevant impact on the confidentiality and availability of information about the asset and stored on the asset's systems, but it did not materially disrupt the provision of essential services. • This must be reported to the ASD's ACSC within 72 hours of IT identifying the malware infection. • You may need to consider whether you have ransomware payment reporting obligations under the *Cyber Security Act 2024*. For guidance visit **Ransomware Payment Reporting Guidance**.
Other Incident #2 – Confidentiality of information	
Circumstances	• A team member of a university is alerted by their IT service provider of unusual activity on their work account, in which their credentials were used to attempt to access and modify sensitive operational data on the entity's secondary data storage systems, including details of contracts and research. Although the files appeared to be uncorrupted, the IT team was able to substantiate that the account had been compromised by an actor who had attempted to view sensitive business critical data that may impact integrity and confidentiality of the asset's function and supply chain, if used maliciously.
Actions	• This would be considered an "other" type of reportable incident as it has had a relevant impact on the confidentiality of information about the asset and stored on the asset's systems, but it did not materially disrupt the provision of essential goods and services. • This must be reported to the ASD's ACSC within 72 hours of becoming aware that the team member's email had been compromised.
Other Incident #3 – Negligent insider incident	
Circumstances	• A team member of a broadcasting asset sends an email to their personal email account. The email contains sensitive and confidential information about the critical infrastructure assets operations. • The IT team were able to contact the employee and request all data is permanently deleted. The employee signs a statutory declaration declaring that the files were deleted and not shared onward.

Actions	• This would be considered an “other” type of reportable incident as it has had a relevant impact on the confidentiality of information about the asset, but it did not materially disrupt the provision of essential goods and services This must be reported to the ASD’s ACSC within 72 hours of IT identifying the data spill.
Other Incident #4 – Service provider incident	
Circumstances	• A service provider experiences a hardware failure. The result is state-wide impact on service provision, impacting over 10 different responsible entities and their critical infrastructure assets. • The service provider enacts their business continuity plans and the result is there is no loss of service. Backed up data is restored, and there is no subsequent data loss.
Actions	• This would be considered an “other” type of reportable incident as it has had a relevant impact on the reliability and availability of information about the asset and stored on the asset’s systems, but it did not materially disrupt the provision of essential goods and services. • This incident must be reported by all impacted responsible entities. In total, 11 reports should be submitted. • This must be reported to the ASD’s ACSC within 72 hours of IT identifying the hardware failure.
Other Incident #5 – Service provider incident	
Circumstances	• Company X is not a responsible entity for a critical infrastructure asset. Company X designs a critical system for the responsible entity of a critical infrastructure asset (Company Y). • Company X experiences a data breach, and the designs for the critical system are leaked as a result. • Company X informs Company Y that the designs have been leaked.
Actions	• This would be considered an “other” type of reportable incident as it has had a relevant impact on the confidentiality of information about the asset, but it did not materially disrupt the provision of essential goods and services. • This incident should be reported by the responsible entity, who would be considered to have become aware of the incident from when Company X informed them the designs were leaked. • This must be reported by Company Y to the ASD’s ACSC within 72 hours of Company X informing Company Y that the designs were leaked.

Other Incident #6 – Service provider incident	
Circumstances	• A malicious actor breaches a data storage or processing provider's network and obtains the schematics of a critical infrastructure asset. • The malicious actor attempts to extort the responsible entity of the critical infrastructure asset. The extortion alerts the responsible entity of the data breach.
Actions	• This would be considered an "other" type of reportable incident as it has had a relevant impact on the confidentiality of information about the asset, but it did not materially disrupt the provision of essential goods and services. • This must be reported to the ASD's ACSC within 72 hours of the attempted extortion.

Questions

For further information please contact us at: enquiries@cisc.gov.au

Australian Government
Department of Home Affairs

CRITICAL
INFRASTRUCTURE SECURITY
CENTRE