Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Mandatory Cyber Incident Reporting

Initial guidance for Critical Infrastructure Sectors

Responsible entities for critical infrastructure assets* have an obligation to report certain types of cyber security incidents under the *Security of Critical Infrastructure Act 2018.*

Why is reporting important?

It gives the Australian Government a **fuller picture of emerging cyber threats and risks**, so they can **better work in partnership with you and other industries** to educate and mitigate against cyber attacks that can seriously impact critical services and businesses.

Your reports will also **help us support you to respond to serious cyber incidents, through helping the Australian Government provide you with timely advice.** This will help you to continue to provide your essential services that our community and economy rely upon.

Something has happened – what should I do?

First, **identify whether a cyber security incident has occurred, is occurring or is imminent.** Cyber security incidents are any of the following:

- Unauthorised access to computer data or program. This includes to secondary data storage systems storing certain business critical data;
- Unauthorised modification to computer data or a computer program;
- Unauthorised impairment or electronic communication via computer; or
- Unauthorised impairment of the availability, reliability, security or operation of a computer, computer data or a computer program.

This obligation applies to data storage systems when:

- vulnerabilities, impacts or access to these systems could have an impact on the availability, integrity, confidentiality or reliability of the critical infrastructure asset
- they are used (or will be used) in connection with the main critical infrastructure asset, and
- you are the responsible entity for the critical infrastructure asset or operate the data storage system.

Second, assess whether the incident has had a **significant or relevant impact** on your asset. Consider your operations, response to the incident and the services you provide. Responsible entities **must report** incidents that either:

Responsible entities for critical infrastructure assets are typically entities who have the licence to own and operate the asset. However, please consult the specific definitions here.

Meet the threshold of 'critical':

with a **significant impact** on the availability of your asset, occurring where:

- Your asset provides essential goods and services; and
- The incident has caused a material disruption to the availability of those essential goods and services.

Indicators of **significant impact** 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.

If a critical cyber incident has occurred, you must report it **here** within **12 hours** of **becoming aware** of the incident.

OR meet the threshold of an 'other' type of reportable cyber security incident:

with a **relevant impact** on the availability, integrity or reliability of your asset, or the confidentiality of information about or stored in your asset.

This includes **imminent** incidents, with a likely relevant impact.

Indicators of **relevant impact** 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 an 'other' cyber incident has occurred, you must report it **here** within **72 hours** of **becoming aware** of the incident.

- Availability means that authorised persons have access to information when and as needed.
- Integrity means that information is only being created, amended or deleted by the intended authorised means and is correct and valid.
- Confidentiality means that only authorised persons should be able to see the information.
- Reliability means the ability of a system or component to function under stated conditions for a specified period of time

Becoming aware means having knowledge of the incident e.g. have you or an employee observed unauthorised access, malicious activity or suspicious outages, resulting in a significant or relevant impact?

Oral reports can also be made via 1300 292 371 (1300 CYBER1). However, they must be accompanied by a written report via the above forms within **84 hours of the initial verbal report** for **critical** incidents and within **48 hours** for **other** incidents. Reports are made to the Australian Cyber Security Centre (ACSC).

**excluding space, defence industry and certain aviation assets*

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Mandatory Cyber Incident Reporting

Initial guidance for Critical Infrastructure Sectors

What do I have to provide in my report?

Contact details: Individual and organisational details.

Incident details: Date and time the incident was identified, which systems are being impacted and whether they are critical to the functioning of your business, description of the impact on the asset, any known information regarding the cause and any commenced or intended response.

- Click **YES** to *'is your organisation part of a critical infrastructure sector?'*
- Clicking **YES** to *'do you consent for this cyber incident report to be provided to the Department of Home Affairs to meet mandatory regulatory reporting requirements?*

We want to know:

- ✓ Can you still provide essential goods and services?
- ✓ Which systems have been taken offline, if any?
- ✓ Initial estimate of impact, including duration of outage

We acknowledge that you may not be able to provide all of this information at the time of making a report.

What might a reportable incident look like?

Case Study 1

- 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.

- This would be considered a **critical** cyber security incident as it has **resulted in material disruption to essential goods and services.**
- This should be **reported to the 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.

Case Study 2

- A team member at a critical infrastructure entity goes to open an **internal planning document,** relating to the asset and finds that it, along with thousands of related files, have been encrypted and they cannot access them. They contact IT and IT 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 essential goods and services, which continue functioning as normal.

- 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 **should be reported to the ACSC within 72 hours of IT identifying the malware infection.**

What might a reportable incident look like?

Case Study 3

- A team member of a critical infrastructure entity 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 entities' 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.

- 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 **should be reported to the ACSC within 72 hours of IT identifying the account compromise.**

Case Study 4

- A team member of a critical infrastructure entity sends an email to their personal email account. The email contains sensitive and confidential information about the critical infrastructure assets operations.
- The team member travels overseas. Subsequently the email cannot be deleted immediately and it cannot be confirmed that the files have not been shared more publicly.
- 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.

- 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 **should be reported to the ACSC within 72 hours of IT identifying the data breach**

Case Study 5

- 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.

- 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 incident should be reported by all impacted responsible entities. In total 11 MCIRs should be submitted.
- This **should be reported to the ACSC within 72 hours of IT identifying the account compromise.**

Sector specific examples are provided at the end of this document

Mandatory Cyber Incident Reporting

Initial guidance for Critical Infrastructure Sectors

Incidents that are generally NOT reportable:

- **Scam calls and emails:** these are only reportable incidents if they lead to further infiltration of computer data or programs, resulting in unauthorised access modification or impairments to computer systems or information.
- **Telephone denial-of service (TDoS) attacks:** these may amount to unauthorised impairment but not via computer. However, if your telephone systems are connected to your broader computer networks, this may amount to a reportable cyber security incident.
- **Social engineering and suspicious contacts**: these are only reportable if 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 secondary data storage systems that *are not* integral** to the availability, integrity, confidentiality or reliability of the critical infrastructure asset.

You should take steps to protect your people, information and assets against threats like these, however, you do not need to report them for SOCI purposes unless they have a significant impact or relevant impact on an asset.

What if I don't report?

- If you don't report, or you don't include sufficient information, we can't help you and other businesses and organisations across Australia protect yourselves or recover as quickly from attacks – which will **hurt our community and economy**.
- You may also be subject to enforcement action such as fines and penalties, as detailed in the Act.
- If you are unsure, you should report even if you have limited information about the incident.

How will the CISC approach compliance?

- The CISC will seek to work in **partnership with industry**, to ensure regulated entities understand and manage their own risk, **encouraging voluntary compliance.**
- The CISC will focus on education and working with entities to understand the reporting thresholds as they relate to each sector. Enforcement action will only be for **egregious breaches** of reporting obligations, such as failure to report critical incidents.

Where can I find out more?

- If you are still unsure whether you need to report an incident or not, or would like further information, contact the Cyber and Infrastructure Security Centre on enquiries@cisc.gov.au or 1300 272 524 (Monday - Friday 9:00am - 5:00pm AEST).

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Mandatory Cyber Incident Reporting

Initial guidance for Critical Infrastructure Sectors

What might significant and relevant impacts look like in my sector?

The following examples represent types of impacts from cyber security incidents that could be considered 'significant' or 'relevant' for assets in each sector. The impact of a cyber security incident will always be dependent upon the impact to your critical asset(s), your operations, response to the incident and the services you provide.

Please note, this guidance reflects the Centre's preliminary view and is provided as examples only. The Centre will work with industry and ACSC through administration of cyber incident reporting and broader engagement to refine these examples over time.

Energy and Water

Significant impact:

- You are unable to provide the essential services that your critical asset provides (e.g. electricity, gas, water, or liquid fuels).
- Your operational technology or ICT is taken offline meaning you cannot control the distribution of your services.
- Your customer data is locked, meaning you stop providing services from your asset because you cannot invoice.

Relevant impact:

- Supply is not disrupted, but you have to put in place workarounds to ensure supply (availability).
- Site plans are accessed (confidentiality).
- Dispatches are being monitored by an unauthorised party (integrity), however, services are able to be provided.
- Customer data is changed or deleted, or invalid invoices are sent (integrity).

Communications

Significant impact:

- You are unable to provide phone, mobile or internet services, likely to result in large outages for consumers and businesses that use your services, meaning they cannot function.
- Being unable to provide your broadcasting services, resulting in disruption to the provision of information.

Relevant impact:

- Services are not disrupted, but you have to put in place workarounds to ensure provision of services (availability).
- An unauthorised party is attempting to disrupt broadcasting (integrity).
- Customers are unable to log in or access support services, however phone service is unaffected.

Data storage and processing

Significant impact:

- Being unable to provide the essential services you provide e.g. cloud services.
- Needing to suspend all access to cloud data to quarantine the impact of unauthorised access to that data.

Relevant impact:

- Critical data is unable to be accessed from the primary server or centre, but there are backup locations (availability).
- Data stored in the cloud or information about asset e.g. locations of data centres, has been accessed by, leaked or tampered with by an unauthorised user, resulting in lost consumer confidence or location vulnerabilities that can be capitalised on by malicious actors in the future (integrity and confidentiality)

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Mandatory Cyber Incident Reporting

Initial guidance for Critical Infrastructure Sectors

What might significant and relevant impacts look like in my sector? (continued)

Financial services and markets

Significant impact:

- A complete outage any essential services provided e.g. banking services, ATMs, POS etc.
- A critical system you operate that powers the stock market is taken offline, meaning no one can trade.

Relevant impact:

- Customer data e.g. bank account details have been leaked or accessed by an unauthorised party (integrity and confidentiality).
- A corporate system linked to core banking assets (e.g. online support) has been subject to a cyber attack. At this stage banking services are unaffected.

Healthcare and medical

Significant impact:

- ICU equipment and systems being disrupted, including backup systems, to the point that critical medical care is unable to be provided to patients.
- Hospital computer systems unable to be accessed, resulting in the transferring of patients and the postponing and cancelling of appointments.

Relevant impact:

- Some equipment and systems connected to the ICU are disrupted or unable to be accessed, but the provision of critical medical care is able to continue, due to segmentation or backup systems etc. (availability).
- Hospital equipment is being remotely tampered with or infected with malware (reliability and integrity).
- Patient data has been tampered with, leaked or accessed by an unauthorised party (confidentiality and integrity).

Food and grocery

Significant impact:

- Being unable to provide the essential good or service that you provide e.g. you are unable to stock the shelves, resulting in food shortages for households and hospitality businesses.
- The temperature control systems in an asset's distribution centre are taken offline, resulting in the spoiling of all produce and severe food shortages for online orders.
- Staff cannot access POS, meaning no stock can be sold and stores are closed as a result.

Relevant impact:

- Information e.g. warehouse inventories or supply chain data has been accessed or tampered with by an unauthorised party (integrity and confidentiality).
- Customer data that has been accessed by an unauthorised party and subsequently leaked.
- Corporate systems impacted and material information leaked.

Transport

Significant impact:

- Ports or airports are unable to be used or must operate at significantly reduced function.
- The trains are unable to run to transport freight, likely to result in practical, negative downstream effects for other sectors of the economy e.g. fuel, medical and agricultural supplies are unable to be transported.

Relevant impact:

- Data within logistics systems has been inappropriately accessed through a cyber attack, however, there is no known impact to operations (integrity and confidentiality).
- Access to billing systems is intermittent due to a cyber attack (availability and reliability).