Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Supporting Australian organisations through a cyber security incident

Table of contents

Supporting Australian organisations

Malicious cyber activity continues to pose a significant risk to Australia's security and prosperity. The persistence of malicious cyber actors, combined with emerging technologies, means that Australian government organisations, critical infrastructure, businesses and households continue to be targeted.

Australian organisations that have been, or may be impacted by a cyber security incident, are encouraged to reach out to the Australian Signals Directorate (ASD). ASD's Australian Cyber Security Centre (ACSC) is the Australian Government's technical authority on cyber security. We offer technical incident response advice and assistance, 24 hours a day, 7 days a week.

This publication is intended for individuals who lead or are involved in an organisation's incident response.

Reporting a cyber security incident to ASD

What types of cyber security incidents should you report to us?

Cyber security incidents[1] can be reported to ASD via www.cyber.gov.au, or the Australian Cyber Security Centre Hotline on **1300 CYBER1** (1300 292 371).

Types of incidents you should report include, but are not limited to:

- Denial of service
- Scanning and reconnaissance
- Intentional or malicious unauthorised access to network or device
- Data exposure, theft or leak
- Malicious code/malware
- Ransomware
- Phishing/spear-phishing
- Other irregular cyber activity that causes concern.

Timeliness is an important factor when managing a cyber security incident, so the earlier you report the better. Even if you're unsure if what you're experiencing is an actual cyber security incident, we still recommend that you report to us as soon as possible.

1 A cyber security incident is a single or series of unwanted or unexpected event(s) that impact the confidentiality, integrity or availability of a network or system or the information that it stores, processes or communicates.

What happens when you report?

ASD is not a regulator, and providing information to us may not itself meet the regulatory obligations that you may have with the Australian Government. More information on reporting and compliance, including mandatory cyber incident reporting, can be found on the Australian Government's Single Reporting Portal: Single Reporting Portal | Cyber.gov.au.

When you report, you will receive immediate incident response advice and assistance which may include:

- information on how to contain and remediate the cyber security incident
- advisory products to assist you with your incident response
- linking you to Australian government organisations that may further support your response
- triaging the incident to determine if there are more detailed actions to be undertaken.

If we assess that your incident requires a more detailed approach, depending on the incident, we may offer:

- a team of digital forensics specialists to support a comprehensive technical investigation
- to work alongside you to liaise and coordinate technical briefings with other government agencies or industry partners to support your response. This could include the federal/state/territory government chief information security officers, federal law enforcement and international cyber partners
- guidance on approaching your public communications to ensure transparency while protecting the integrity of the technical investigation–this is separate to the whole of Australian Government and consequence management communications that is led by the National Office of Cyber Security (NOCS)
- information and reports to help you finalise your investigation. These products will be provided by ASD on a case by case basis
- to introduce you to different areas within ASD for additional support such as cyber resilience uplift activities, and if requested, assist you to contact the NOCS or Australian Federal Police.

Working with your incident response provider or legal representative

Where an organisation has engaged the services of an incident response provider, or legal representative, we will work collaboratively with them to establish the full nature and extent of your incident. This collective approach to sharing technical expertise, threat intelligence and capabilities strengthens and provides a more comprehensive investigation into the cyber security incident.

The success of this collaboration however, relies on your organisation's authorisation to share information between ASD and your incident response provider or legal representative.

Information provided to us by your legal representative or incident response provider is covered under Limited Use. More details on Limited Use is outlined below, under *How ASD protects your privacy*.

What ASD may need from you when you report

We are here to help your organisation respond to the technical aspects of the incident. To do so, we may request that you share, where available, evidence of malicious activity. This can include:

- Logs
- Memory dumps
- Disk images
- Network traffic captures
- Network diagrams/documentation
- Indicators of compromise
- Samples of malware
- Other analysis or reporting products.

ASD can also discuss possible tools to assist with provision of these artefacts, along with a secure means to transfer them to us. While these requests can seem resource intensive, the more information you can pass to us in a timely manner, the more effective our support to you will be. Where possible, we will enrich your cyber security incident data with our unique accesses and threat intelligence insights which allows for a wider perspective on the investigation.

Other questions ASD may ask

1. Do you have a Cyber Incident Response Plan? Has this been implemented? And can this be shared?
2. Do you have technical resources (including an incident response provider) readily available to investigate and mitigate an incident? Can you provide their contact details?
3. What actions have been taken so far, why and how have you recorded this? What steps have been taken to contain the threat? Is the threat actor still on your systems?
4. Do you have the ability to identify and isolate an affected workstation or system?
5. What are your next steps for investigating and mediating this incident?

What if you are contacted by ASD?

We obtain cyber threat information through numerous trusted sources, and through our own monitoring of the cyber threat environment. From this, we may contact you if we discover a vulnerability, potential compromise or a confirmed compromise that could impact your organisation, such as:

- indicators of compromise
- compromised credentials
- ransomware precursor activity (i.e. from detection of malware or spear phishing activity)
- interactions between malicious infrastructure and Australian networks or devices.

If you're contacted by ASD's ACSC, we will always provide you with an incident/reference number. If you're concerned about the legitimacy of a call, you can verify that you were speaking to a genuine ASD representative by calling the Australian Cyber Security Hotline (1300CYBER1) and quoting your incident/reference number.

If you are an ASD Partner, ensure your contact details are up to date and you've registered 'out of hours' contact details so we can contact you quickly.

Remember to respond to ASD

When we engage with your organisation, we ask that you respond, even if the notification doesn't end up being a compromise. That way we can ensure we provide you with prompt support if needed.

How does reporting your incident help others?

One of ASD's key strengths is our ability to aggregate and analyse information to produce a national cyber threat picture. We draw upon information gathered through our intelligence sources and crucially, the information provided by organisations impacted by cyber security incidents in Australia.

We use this understanding to assist with developing new and updated cyber security advice, capabilities, and techniques to better prevent and respond to evolving cyber threats. For example, anonymised information from your incident may be used to produce public communication products to help build whole of economy cyber resilience. Products could include:

- Advisories published on the Partner Portal
- Alerts published on cyber.gov.au
- Quarterly Trends and Insights reports
- Annual Cyber Threat Report
- Some anonymised technical details, such as indicators of compromise can also be shared via our Cyber Threat Intelligence Shared (CTIS) platform.

Improved cyber security through information sharing

At the end of 2023, a malicious cyber actor compromised an internet-facing server used by an Australian critical infrastructure (CI) organisation. The CI organisation immediately notified ASD. The CI organisation agreed to activate additional log data to better observe the actor's activity. These observations provided valuable insight into actor tradecraft, capability and lateral movement.

The CI organisation shared with ASD log data along with a disk and memory image from the compromised server to enable joint analysis. This provided ASD with useful details to improve our understanding of the malicious cyber actor's tactics, techniques and procedures. This helped to create new detection rules, which were shared with the CI organisation, and could also be used to protect other Australian organisations from similar activity.

ASD takes information we learn from conducting investigations like this to feed our Cyber Threat Intelligence Sharing (CTIS) platform and AUPDNS. CTIS is a two-way sharing platform that enables government and industry partners to receive and share information about malicious cyber activity at machine speed and Australian Protective Domain Name Service (AUPDNS) is a free opt-in security service available to all federal, state and territory government entities. ASD partners who opt in to CTIS and AUPDNS directly benefit from the national cyber threat picture that ASD collates from investigations like this, as well as ASD's other threat intelligence sources

Protecting our Australian community from cyber threats is a team effort. This example of collaboration and information sharing shows just some of the mutual benefits that can be achieved.

How ASD protects your privacy – Limited use obligation

The limited use obligation has been legislated to add additional protections to the information organisations provide to ASD about cyber security incidents and potential incidents, including vulnerabilities.

Under the limited use obligation, information voluntarily provided by an impacted entity to ASD, or information acquired or prepared by ASD with the consent of an impacted entity, about a potential or actual cyber security incident, cannot be communicated or used for the purposes of any civil claims or regulatory investigations or enforcement against the impacted entity.

- The limited use protections extend to information provided to ASD by entities engaged to act on behalf of the impacted entity. This could include legal representatives or incident response providers.

ASD is not permitted to provide limited use information to a regulator for the purposes of investigating or enforcing a regulatory or civil offence against the impacted entity. If a regulator requests cyber security incident information for these purposes, ASD will advise them to contact the organisation in question. We will not confirm or deny that an incident has occurred.

ASD staff members, both former and current, cannot be compelled to comply with a subpoena or similar court direction to attend and answer questions relating to information protected by the limited use obligation.

Limited use information in the hands of a Commonwealth, State or Territory body is not admissible in Commonwealth, State or Territory criminal or civil proceedings, with some limited exceptions. These exceptions include:

- section 137.1 and 137.2 of Criminal Code (false or misleading information or documents)
- section 149.1 of Criminal Code (obstruction of Commonwealth officials)
- a civil offence regarding a breach of Limited Use provisions
- a coronial inquiry or royal commission.

Limited use is not intended to be a 'safe harbour' to shield industry from legal liability. The limited use obligation aims to strike a balance between providing assurance to industry to encourage open and early engagement with ASD, and protecting broader public interests by not impeding appropriate regulatory activity.

Limited use does not restrict regulators or law enforcement agencies from seeking information relating to a cyber incident directly from an impacted entity by means of their own information gathering powers.

To learn more about how ASD protects your information under Limited Use, visit Limited Use.

ASD's role in whole of government cyber security incident response

ASD is the Commonwealth lead for technical cyber incident response and advice for cyber security incidents. We also work closely with other partners including the National Cyber Security Coordinator. While ASD is not a law enforcement agency, we also work closely with the AFP Cyber Command under the standing joint counter cybercrime Operation Aquila. If you refer your incident to the AFP for criminal investigation, we can work collaboratively with the AFP to support your investigation. ASD can also assist you in engaging AFP Cyber Command support.

Becoming an ASD Partner

Sign up for ASD's free cyber security services to reduce your exposure to threats. Connect with ASD through a click of a link on the Partner Portal. As an ASD Network Partner you may be provided access to:

- threat intelligence, news and advice to enhance situational awareness
- collaboration opportunities
- resilience-building activities (e.g. exercises, discussions, workshops)
- ASD's State and Territory network.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre