Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

ASD's role in cyber security: For legal practitioners

First published: 10 December 2024

The Australian Signals Directorate (ASD) defends Australia from global threats and advances the national interest by providing foreign signals intelligence, cyber security and offensive cyber operations, as directed by the Australian Government.

ASD's functions set out in the *Intelligence Services Act 2001* (ISA) include, among other things, preventing and disrupting, by electronic or similar means, cybercrime undertaken by people or organisations outside Australia.

ASD's role in cyber security

The Australian Cyber Security Centre (ACSC) is part of ASD, the Australian Government's technical authority on cyber security. The ASD's ACSC's remit includes:

- the Australian Cyber Security Hotline, which is contactable 24 hours a day, 7 days a week, via 1300 CYBER1 (1300 292 371)
- publishing notifications, alerts and advisories on significant cyber threats on the cyber.gov.au website and ASD's Partner Portal
- publishing technical advice for individuals, small to medium businesses, large enterprises and government on the cyber.gov.au website
- cyber threat monitoring and intelligence sharing with partners
- helping Australian organisations respond to cyber security incidents
- conducting exercises and uplift activities to enhance the cyber security and resilience of Australian organisations
- supporting collaboration between Australian organisations and individuals on cyber security issues through ASD's Cyber Security Partnership Program.

Working with ASD during a cyber security incident

If an organisation experiences a cyber security incident, it is important they report it to ASD as soon as it is detected. Even if the organisation is unsure if what they have experienced is an actual cyber security incident, it is still important to report it.

Reporting the right amount of information, at the right time to ASD ensures we can provide the impacted organisations with the appropriate technical support and advice. We will also harness our unique cyber threat intelligence insights to support organisations in recovering and restoring their business operations.

While ASD welcomes the opportunity to work with an impacted organisation's legal representation, information exchanges that are timely and technically comprehensive assist us to best assist impacted entities. Delays in the exchange of technical details can delay investigation or recovery efforts.

ASD is not a government regulatory body. During a cyber security incident, or suspected cyber security incident, our goal is to work with impacted organisations, their legal representation, and any external vendors engaged to investigate an incident on behalf of the organisation to:

- determine the extent of the cyber security incident, the nature of the adversary, their sophistication and their intent
- where possible, enrich organisations' understanding of their cyber security incident with our unique accesses and insights (this enables ASD to look at the activity from a wider perspective to help contextualise what your client is seeing. By exploring all available avenues, our investigation is robust. This gives us a better chance to detect the adversary's activity across the impacted organisation's network)
- support organisations to mount an effective response to a cyber security incident so that their network, and Australian networks more broadly, can operate securely
- develop and maintain a comprehensive national cyber threat picture
- extract tactics, techniques and procedures, and indicators of compromise, and input them into ASD's tools to protect the nation.

Information ASD may request

ASD requires certain information to perform its cyber security role, including:

- technical incident information
- technical network telemetry
- knowledge of cyber security related vulnerabilities (i.e. information on the nature of the breach, including whether the threat actor used specific software or known access vectors).

Handling cyber security incident information – Limited Use

When ASD shares cyber security incident information in accordance with its statutory functions, the information will typically be aggregated or completely anonymised. When engaging in uplift activities, ASD's focus is on the potential sectors or threat vectors that need attention, not the identity of an impacted organisation. If an entity is reasonably identifiable from the information we share, the information will generally be protected under the limited use obligation.

What is Limited Use?

- 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.

What is excluded from Limited Use?

- Limited use does not override an organisation's mandatory reporting obligations, and information provided by an impacted entity for mandatory reporting purposes is excluded from the regime.
- If information has been made publicly available through lawful means, it is excluded from the protections offered by the obligation. For example, if the impacted entity publicly discloses the information protected by limited use.
- Limited use does not apply to information that is de-identified to not reasonably identify an entity.

Does Limited Use information expire?

- The limited use protections are perpetual and will not expire.
- However, if information is lawfully made public, then limited use will no longer apply to that information.

What happens if someone breaches limited use?

- Offenders are liable for a civil penalty of 60 penalty units.
- Commonwealth officers are subject to standard secrecy provisions such as the Criminal Code or Intelligence Services Act.

Activities outside ASD's remit

It is outside ASD's remit to conduct offensive cyber activities to support organisations' cyber security incident investigations or remediation efforts.

While ASD does conduct offensive cyber activities, this is only done in very specific circumstances in support of Australian Government national security priorities. ASD's offensive cyber operations require explicit authorisation from the Australian Government. These operations are subject to rigorous oversight, review processes and strict adherence to legal, ethical and operational guidelines.

Rules and legislation

There are several important rules and legislation that apply to ASD's operational activities.

- The ISA outlines ASD's functions, limits and conduct. Any activity ASD conducts must fall under one of the functions specified in section 7 of the ISA and must be within the limits set out in sections 11 and 12 of the ISA.
    - Section 15 of the ISA requires the Minister for Defence to create rules regulating the communication and retention by ASD of intelligence information concerning Australian persons. In making the rules, the Minister must have regard to the need to ensure that the privacy of Australian persons is preserved as far as is consistent with the proper performance by ASD of its functions. The Rules to Protect the Privacy of Australians can be found on the ASD website.
    - Division 1A of the ISA contains the provisions setting out the limited use obligation, including:
        - limitations on secondary use and communication of limited cyber security information (as set out by sections 41BB and 41BC);
        - restrictions on use and communication of limited cyber security information for civil or regulatory investigation or enforcement (as set out in subsections 41BB(2) and 41BC(3)); and
        - penalties for breach of the limited use obligations (as set out in section 41BC (6)).
- The *Telecommunications (Interception and Access) Act 1979* focuses on protecting the privacy of Australians with regards to Australian telecommunications networks. It does this by setting strict guidelines about what is legal and what is not with regards to intercepting and accessing communications data off such networks.
- Part 5.6 of the *Criminal Code Act 1995* establishes Commonwealth criminal offences which apply to employees and contractors of ASD and certain other individuals when they breach the secrecy of information.
- ASD is exempt from requests made under the *Freedom of Information Act 1982* and this extends to the information that has originated with, or has been received from, ASD.
    - This exemption continues to apply to documents ASD shares with other Commonwealth entities. Such entities are expected to consult ASD when they receive any FOI requests involving ASD documents.

Further information

- For more information on the support provided by ASD during a cyber security incident, refer to *How the ASD's ACSC can help* during a cyber security incident.
- For more information about limited use, refer to the limited use page on cyber.gov.au.
- To help organisations meet their cyber reporting requirements, the Australian Government's Single Reporting Portal provides a list of Commonwealth legislative reporting requirements that could be triggered by a cyber security incident.