SANCTIONS GUIDANCE NOTE

CYBER SANCTIONS

FRIST PUBLISHED: 20 DECEMBER 2023 - LAST UPDATED: 6 DECEMBER 2024

This guidance note is produced by the Australian Sanctions Office (ASO) within the Department of Foreign Affairs and Trade (DFAT). It provides a summary of relevant sanctions laws but does not cover all possible sanctions risks. Users should consider all applicable sanctions measures and seek independent legal advice. This document should not be used as a substitute for legal advice. Users are responsible for ensuring compliance with sanctions laws.

OVERVIEW

Australia is experiencing an increase in persistent and pervasive cybercrime threats targeting critical infrastructure, governments, industry and the Australian community. The Government will use all lawful and appropriate levers to deter and disrupt cybercrime. Australia's autonomous sanctions framework, which is established by the *Autonomous Sanctions Act 2011* and the *Autonomous Sanctions Regulations 2011* (collectively, 'Australian autonomous sanctions laws') is one tool available to respond to a significant cyber incident.

This Guidance Note outlines the following:

- Australia's cyber sanctions framework,
- compliance obligations under autonomous sanctions law, including the need to undertake due diligence,
- the risks associated with making or facilitating a ransomware payment to persons or entities subject to sanctions.

Contents

GLOSSARY

Term	Definition
Australian Sanctions Office	The Australian Sanctions Office (**ASO**) is the Australian Government's sanctions regulator. The ASO sits within the Department of Foreign Affairs and Trade (**DFAT**).
Consolidated List	See **Designated person or entity**.
Controlled asset	Generally an asset owned or controlled by a designated person or entity. Some sanctions legislation also refers to these kinds of assets as 'freezable assets'.
Designated person or entity	A person or entity listed under Australian sanctions laws. Listed persons and entities are subject to targeted financial sanctions. Listed persons may also be subject to travel bans. See DFAT website for further information. Some sanctions legislation also refers to these persons and entities as 'proscribed persons and entities'. DFAT keeps a Consolidated List of designated persons and entities, available on the Department's website.
Pax	Pax is the Australian sanctions platform. You can make general enquiries or submit sanctions permit applications to the ASO in Pax.
Reasonable precautions and due diligence	In the sanctions context, reasonable precautions and due diligence are not defined terms but generally refer to the steps and measures a regulated entity must take to ensure it is not engaging in sanctioned activities. This includes implementing robust internal controls, screening transactions and parties against the Consolidated List, and ensuring staff are adequately trained to recognise and respond to potential sanctions risks. This is a relative standard, as what constitutes "reasonable" can vary based on a range of factors, including the size and nature of the business, the complexity of transactions, the geographic areas involved, and the specific sanctions regulations in place. Consequently, what is deemed sufficient for one entity may not be for another, making the concept inherently flexible and context dependent.
Regulated entity	A government agency, individual, business or other organisation whose activities are subject to Australian sanctions laws.
Sanctions permit	A sanctions permit is authorisation from the Minister for Foreign Affairs (or the Minister's delegate) to undertake an activity that would otherwise be prohibited by an Australian sanctions law.

OVERVIEW OF AUSTRALIA'S CYBER SANCTIONS FRAMEWORK

Australia established a thematic autonomous sanctions framework on 21 December 2021 in relation to significant cyber incidents. The purpose of this framework is to disrupt and frustrate the perpetrators of malicious cyber activity and not to punish victims of crime.

The Minister for Foreign Affairs may impose a cyber sanction if satisfied that a person or entity has caused, assisted with causing, or been complicit in, a cyber incident or an attempted cyber incident that is significant or which, had it occurred, would have been significant.

A cyber incident may include events that result in harm to individuals, businesses, economies or governments. The conduct amounting to a significant cyber incident or attempted cyber incident could have occurred anywhere in the world outside of Australia.

What constitutes a 'significant cyber incident' will be determined on a case-by-case basis. Guidance is provided in the *Autonomous Sanctions Regulations 2011* as to matters the Minister for Foreign Affairs may have regard to in deciding whether a cyber incident was, or would have been, significant.

Once sanctioned, a person or entity is referred to as a 'designated person' or 'designated entity'.

Who must comply with Australian autonomous sanctions laws?

Autonomous sanction laws apply to those conducting activities:

- in Australia,
- by Australian citizens and Australian-registered bodies corporate overseas,
- on board Australian-flagged vessels and aircraft.

The Minister for Foreign Affairs, or the Minister's delegate, may grant a sanctions permit authorising certain activities that would otherwise contravene Australian sanctions laws, if satisfied that it is in the national interest to do so (more information is available at About sanctions).

In addition to Australian autonomous sanctions laws, consideration should also be given as to whether any activity you intend to engage in is subject to other Australian laws or the sanction laws of another country. If so, it is recommended you seek legal advice as to how those laws may impact upon the activity.

Penalties for sanctions offences

Sanctions offences are punishable by:

- For an individual - up to 10 years in prison and/or a fine of 2500 penalty units ($825,000 as of 7 November 2024) or three times the value of the transaction(s) (whichever is the greater).
- For a body corporate – a fine of up to 10,000 penalty units ($3.3 million as of 7 November 2024 or three times the value of the transaction(s) (whichever is the greater).

The offences are strict liability offences for bodies corporate, meaning that it is not necessary to prove any fault element (intent, knowledge, recklessness or negligence) for a body corporate to be found guilty. However, an offence is not committed if a body corporate proves that it took reasonable precautions, and exercised due diligence, to avoid contravening the autonomous sanctions laws.

There are practical steps you can take to ensure you (and/or your business) are in compliance with Australian sanctions laws.

What happens when a sanction is imposed in relation a significant cyber incident?

When a sanction is imposed in relation to a significant cyber incident, the designated person or entity is subject to targeted financial sanctions and/or a travel ban.

Targeted financial sanctions prohibit directly or indirectly making an asset (including funds or economic resources, such as crypto assets) available to (or for the benefit of) a designated person or entity.

Targeted financial sanctions also prohibit an asset holder (such as banks or crypto exchanges) from using or dealing with an asset that is owned or controlled by a designated person or entity, or allowing the asset to be used or dealt with, or facilitating the use of the asset or dealing with the asset.

Making or facilitating a ransomware payment to a person or entity subject to a cyber sanction would be a contravention of Australia's sanctions laws. It could expose you to criminal penalties.

Travel bans prohibit a person from travelling to, entering or remaining in Australia.

COMPLIANCE OBLIGATIONS UNDER AUSTRALIAN AUTONOMOUS SANCTIONS LAW

It is your responsibility to ensure you (and/or your business) do not contravene Australian cyber sanctions laws, and you must ensure that there are sufficient measures in place to avoid breaching sanctions. It is recommended that you:

- assess your own level of exposure to Australian sanctions laws,
- seek legal advice,
- put in place due diligence measures to manage any identified or anticipated risk of breaching financial sanctions.

The Australian Sanctions Office (ASO) provides guidance (including the Sanctions Compliance Toolkit) on its website and a checklist on what you can do to ensure you comply with, and reduce your risk of contravening, Australian cyber sanctions laws. To mitigate your risk of breaching Australian cyber sanctions laws, ASO recommends you check the DFAT website to familiarise yourself with your obligations and undertake due diligence.

As part of your due diligence checks, it is important that you inform yourself about persons or entities connected with your proposed activity to ensure you do not contravene Australian cyber sanctions laws. To do this, you can search the Consolidated List. The Consolidated List is a list of all persons and entities who are subject to targeted financial sanctions under Australian sanctions law. Persons listed on the Consolidated List may also subject to a travel ban.

If your proposed activity in any way involves a person or entity listed on the Consolidated List, you should consider seeking legal advice before taking further action.

The ASO is here to assist you to understand your rights and responsibilities and will work with you to prevent and address breaches of Australian autonomous sanctions laws. It cannot, however, provide legal advice or advice on the sanctions laws of other countries, and it does not mandate specific sanctions systems, controls or due diligence measures.

If you have specific questions regarding your situation, please contact the ASO at sanctions@DFAT.gov.au.

Payment of ransomware demands

The Government's focus is on pursuing and deterring perpetrators of malicious cyber activity and the sanctions are directed towards that end. The Government's priority is to assist Australians who find themselves victims of ransomware attacks.

While the Government strongly discourages the payment of ransoms, the focus of the cyber sanctions framework is to disrupt and frustrate the perpetrators of malicious cyber activity, such as ransomware attacks, not to punish victims of crime.

The Government encourages victims of ransomware attacks to approach it for advice. For guidance on how to deal with an attack, please consult the Australian Federal Police (AFP) and Australian Cyber Security Centre (ACSC) via the ReportCyber website.

If you suspect a ransomware payment has been made to a designated person or entity, you should also report this to the ASO as soon as possible, via email at sanctions@DFAT.gov.au through the online portal Pax.

That a victim had engaged with the Government concerning the ransomware attack and/or voluntarily disclosed the fact of the ransom payment would be taken into account in any decision to pursue any enforcement or compliance action.

Tips to comply with Australian autonomous sanctions laws following a cyber incident

- Has a crime been committed that needs to be reported? Report to ReportCyber?
- Have you called the ACSC's 24/7 Hotline on 1300 CYBER1 (1300 292 371) for cyber security assistance?
- Are the persons or entities you are dealing with sanctioned by Australia? Run a check of the names of the persons and entities on the Consolidated List, and sign up to ASO's email distribution for updates to the Consolidated List.
- Have you sought legal advice to understand any sanctions implications for your proposed activities?
- If you operate internationally, are there any other countries sanctions laws you need to consider?

Resources

- DFAT Consolidated List of sanctioned persons and entities
- Submit your questions, potential sanctions breaches, permit requests and compliance issues to DFAT Online Sanctions Portal Pax
- Report a cybercrime, incident or vulnerability at ReportCyber
- ACSC Resources on Ransomware:
    - What is ransomware,
    - Ransomware Emergency Response Guide: One Page Guide,
    - Ransomware Emergency Response Guide: Recover from a Ransomware Attack,
    - Ransomware Prevention Guide.
- DFAT Advisory on Democratic People's Republic of Korea (DPRK) information technology (IT) workers.

Overview of relevant stakeholders

The ASO within the **Department of Foreign Affairs and Trade,** is the authority responsible for implementing Australia's sanctions framework on behalf of the Minister for Foreign Affairs. The ASO:

- provides guidance to regulated entities, including government agencies, individuals, business and other organisations on Australian sanctions law.
- processes applications for, and issues, sanctions permits.
- works with individuals, businesses and other organisations to promote compliance and help prevent breaches of the law.
- works in partnership with other government agencies to monitor compliance with sanctions legislation.

- supports corrective and enforcement action by law enforcement agencies in cases of suspected non-compliance.

The AFP's **Cyber Command** investigate cybercrimes against the Commonwealth Government, critical infrastructure, systems of national significance and matters impacting the whole of Australian economy.

- Combating cybercrime is a key part of the AFP's efforts to protect the Australian community from the direct and indirect impacts of cybercrime, and to make Australia a hostile environment for cybercriminals and syndicates. The AFP work to disrupt anonymous cybercriminals who are using the dark web to evade detection.

The **Australian Signal Directorate's ACSC**, leads the Australian Government's efforts to improve cyber security. Their role is to make Australia to most secure place to connect online. They work with business, government and academic partners and experts in Australia and overseas to investigate and develop solutions to cyber security threats.

The **National Office of Cyber Security**, housed within the Department of Home Affairs, supports the National Cyber Security Coordinator to ensure Australians are better protected against cyber threats; businesses and critical infrastructure entities are cyber resilient; and the delivery of the *2023-2030 Australian Cyber Security Strategy* to make Australia a world leader in cyber security by 2030.

Sanctions permits

The ASO advocates for proactive risk management rather than relying on permits. Sanctions permits are generally appropriate only when there is a clear likelihood of a sanctions contravention occurring. For broad or non-specific sanctions risks, it's better to manage compliance through **reasonable precautions and due diligence** to prevent issues before they arise. To enable due consideration of any permit application, ASO must be provided sufficient detail of a specific contravention to which the application relates.

Further information on sanctions permits and how to apply for a sanctions permit can be found here.

Further information and resources

While this guidance note provides a framework for understanding key sanctions risks and compliance requirements, it is essential to remember that it does not cover every possible scenario. Sanctions compliance is a dynamic, ongoing process rather than a one-time assessment. Sanctions measures and associated risks are constantly evolving, requiring regulated entities to continuously monitor and reassess their compliance strategies. Regulated entities are encouraged to seek independent legal advice tailored to their specific situations and ensure thorough due diligence in all activities.

Further information is available on the Department's website and in ASO guidance notes on specific sanctions topics. If you have any questions, you can make an enquiry through Pax.