SANCTIONS GUIDANCE NOTE

ARTIFICIAL INTELLIGENCE AND QUANTUM TECHNOLOGY SECTOR

DATE: 11 June 2025

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

The ASO is committed to working cooperatively with the regulated community to address sanctions non-compliance. The community plays a key role in reporting sanctions non-compliance to the ASO. The ASO encourages the public to report any instances of sanctions non-compliance they become aware of. This includes reporting non-compliance by others, such as businesses, and self-reporting their own non-compliance.

SANCTIONS RISKS

The rapid advancement and integration of artificial intelligence (AI), along with the potential research of quantum technology, present an increasing risk that Australians and Australian businesses may encounter sanctions risk. This guidance note aims to alert the AI and quantum technology sector to potential sanctions risks in the transfer of assets (including intangible assets) and the provision of a sanctioned service. Ultimately, it is the responsibility of the Australian community to be aware of, and understand, obligations relating to Australian sanctions laws. The ASO recommends that Australians or entities operating in Australia seek independent legal advice prior to engaging in activities that may contravene Australian sanctions laws.

Dealing with designated persons or entities and controlled assets

Australia has imposed prohibitions on dealing with certain persons, entities and assets. The purpose of these prohibitions is to freeze a person's or entity's assets and prevent them from obtaining and/or benefiting from any additional assets while they are subject to targeted financial sanctions.

For the purposes of Australian sanctions laws, an 'asset' includes an asset or property of any kind, whether ***tangible or intangible***, movable or immovable. It can also include a legal document or instrument evidencing title to, or an interest in an asset – e.g., intellectual property, research, electronic material and software.

Targeted financial sanctions generally prohibit:

- directly or indirectly making an asset available to, or for the benefit of, a designated person or entity;
- an asset-holder using or dealing, or allowing or facilitating the use or dealing, with an asset that is owned or controlled by a designated person or entity. As these assets cannot be used or dealt with, they are referred to by the ASO as 'frozen'.

The designated persons and entities on which targeted financial sanctions have been imposed are identified on the Consolidated List.

Sanctions Supply or Potential for military end use

A number of Australia's sanctions frameworks include a prohibition on the supply, sale or transfer of certain goods to another person or country. Depending on the sanctions framework, this may include a prohibition on the supply, sale or transfer of 'arms or related matériel'.

Companies involved in the AI and the quantum technology sector should evaluate whether their products have the potential for military end use. The definition of 'arms or related matériel' under Australia's sanctions laws includes, but is not limited to: weapons; ammunition; military vehicles and equipment; spare parts; accessories for these things; and paramilitary equipment. Goods that do not clearly fall within one of these categories may still be considered 'arms or related matériel'.

Companies involved in the AI and the quantum technology research sector should apply the 'three-step test' to determine if a good is considered 'arms or related matériel'. This is particularly the case where the AI software has specific characteristics that align with controlled 'dual-use' goods or technology, under the relevant dual-use regulations, such as advanced data analytic tools, machine learning processes and cybersecurity software (i.e. items that can have both civilian and military application).

Providing a sanctioned service

Australian sanctions laws impose restrictions on providing certain sanctioned services. Whilst there are a number of common prohibitions, the precise scope of the restrictions depends on the particular sanctions framework. Please refer to the Sanctions Compliance Toolkit for further information.

A number of Australia's sanctions frameworks include prohibitions on providing a 'sanctioned service', which may include, but is not limited to the provision to a person of:

- technical advice, assistance or training,
- financial assistance,
- a financial service, or
- another service,

if it assists with, or is provided in relation to:

- a 'sanctioned supply',
- a 'military activity'; or
- the manufacture, maintenance or use of 'export sanctioned goods' (which may include arms or related matériel).

Please refer to each framework for the specific prohibitions

In the context of a technology company, the prohibition on a 'sanctioned service' will generally apply to:

- the provision of technology or technical advice related to the manufacture, maintenance or use of 'export sanctioned goods'; or the assistance or training if it assists with the manufacture, maintenance or use of an 'export sanctioned good.'

In this context, 'technology' includes specific information about the development, design, production, or 'use' of an export-sanctioned good. The prohibition may apply if the service is provided to the sanctioned country (e.g., a government entity) or to a person (e.g., a citizen or resident) for use in the sanctioned country. It is essential to evaluate the risk of whether the service provided to a business or individual may result in goods being supplied to a sanctioned country. The prohibition on 'technical advice, assistance, or training' also encompasses various types of products, training and knowledge transfer.

In addition to services related to 'export sanctioned goods', 'sanctioned services' also encompass specific restrictions related to particular countries (or parts of countries) and activities which do not require a nexus to an 'export sanctioned good'.

These country-specific sanctioned services apply to countries including Syria, Russia, Zimbabwe, the Democratic People's Republic of Korea (DPRK), and specified regions of Ukraine (Crimea, Donetsk, Luhansk, Sevastopol, and regions specified by the Minister). For example, a sanctioned service for the DPRK also includes engaging in sanctioned scientific or technical cooperation with persons sponsored by or representing the DPRK.

STRICT LIABILITY

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 ($3.30 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 can demonstrate that it took reasonable precautions, and exercised due diligence, to avoid contravening Australia's sanctions laws.

RED FLAGS

- The end receiver is in a business sector that would not typically engage or have use of AI software or quantum computing research.
- The customer (domestic or foreign) has a limited or no online profile and provides little or no explanation of their business interests in the products.
    - The information provided, such as postal or residential address is generic or an on-freighter, and no physical address of the business has been provided.
    - The company's address is co-located with other businesses.
- The customer (or receiving company) has a complex or opaque beneficial ownership structure.
- The business operates in a jurisdiction of high sanctions risks.
- Payment for the products occurs outside the banking sector, including through remittance, cryptocurrency or an alternative payment platform.
- The recorded payee in the transactions appears to be an unrelated company or entity.

POTENTIAL DUE DILIGENCE MEASURES

- Seek to ensure that users are not individuals or entities that are directly or indirectly (by reason of ownership or control) subject to sanctions.
    - Seek information on the customer, including verifying details such as name, title, phone number, email address, date, and signature.
    - Evaluate the customer's corporate structure and details, including date of incorporation and beneficial ownership structure.

    - Evaluate the end user and end use of the item (e.g., whether the customer's line of business is consistent with the ordered items).
        - Consider the potential likelihood of re-export or on selling by the customer.
- Ensure that processes are in place to verify that your AI products are not being used to support sectors/industries, or underlying trade, that may be subject to sanctions restrictions.
    - Consider incorporating end user certificates to prevent the indirect transfer of your product to sanctioned entities or high-risk jurisdiction for sanctions.
- Restrict access to users within high-risk jurisdictions that are subject to comprehensive and/or sectoral sanctions.

FURTHER INFORMATION AND RESOURCES

While this guidance note provides a framework for understanding key sanctions risks and compliance requirements, 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 on their specific situation and to ensure thorough due diligence in all activities.

We recommend users also refer to the following guidance to assist in their evaluation of sanctions risks:

- Sanctions Compliance Toolkit | Australian Government Department of Foreign Affairs and Trade
- Sanctions Risk Assessment Tool | Australian Government Department of Foreign Affairs and Trade
- Guidance Note - Sanctions compliance for universities | Australian Government Department of Foreign Affairs and Trade.

Further information is available on the Department's website at https://www.dfat.gov.au/international-relations/security/sanctions, or by making an enquiry to sanctions@dfat.gov.au.