ADVISORY NOTE

SANCTIONS RISKS FROM MISUSE OF AI AND NEW TECHNOLOGIES

DATE: 06 November 2025

This ADVISORY NOTE is produced by the Australian Sanctions Office (ASO) to inform the regulated community of a developing issue presenting significant sanctions risk. 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 Australian sanctions laws.

Risks posed by the abuse of Artificial Intelligence (AI) and Emerging Technology

Artificial intelligence and other emerging technologies have been recognised as having the potential to be exploited for financial fraud and deception. Such misuse may involve impersonations through voice or video deep fakes, falsified documentation, and the manipulation of records, including personal identification or corporate information. Generative AI (a type of artificial intelligence that creates live new content, such as text, images, videos and code based on user input) can produce convincing and internally consistent sets of fraudulent documents.

Specific Sanctions Risks

There is a concern that AI and emerging technologies could facilitate sanctions contraventions and contribute to complex methods of sanctions circumvention – as noted in the recent FATF report on complex proliferation financing and sanctions evasion schemes. AI can create and oversee extensive networks of false identify (commonly known as synthetic entities), each with distinct digital characteristics and accompanying documentation. This may make it more challenging to associate these entities with a malicious actor.

Falsifying the nature, origin or destination of goods is a common tactic in trade-based money laundering and sanctions evasion. The use of AI technology may increase the sophistication of deceptive conduct used to circumvent trade-based sanctions and export controls. AI may assist in producing realistic fraudulent documents, such as bills of lading, certificates of origin and packing lists, and is a well-established method of sanctions evasion.

Businesses should recognise the risks associated with AI and emerging technologies in relation to sanctions, and review their processes to ensure they are adequately protected. This may include additional verification of documents, the use of AI detection software, and potentially confirming identity of high-risk individuals through face-to-face meetings.

Case study: To avoid detection, DPRK IT workers frequently assume false identities, both fake and stolen, claiming to be from countries with strong tech industries such as South Korea, Japan, China, or Eastern European nations. There are reports that DPRK IT workers are using real-time deepfake technology (including commercially available filters) to obfuscate their true identities.

For more information on this issue please refer to the following public reports

- RUSI Beware the Robots: AI-Enabled Sanctions Evasion is Here | Royal United Services Institute

- FATF Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf

Businesses engaged in AI and quantum technology research may encounter sanctions risks. For further information, the ASO has issued the following guidance note:

- Guidance Note - Artificial intelligence and quantum technology sector | Australian Government Department of Foreign Affairs and Trade

Further information and resources

While this advisory 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 an ongoing obligation 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. Australian regulated entities are encouraged to seek independent legal advice tailored to their specific situations and ensure thorough due diligence in all activities.

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

- Sanctions Compliance Toolkit
- Sanctions Risk Assessment Tool
- Advisory Note - Democratic People's Republic of Korea (DPRK) information technology (IT) workers | Australian Government Department of Foreign Affairs and Trade
- Advisory Note – Sanctions & proliferation financing | Australian Government Department of Foreign Affairs and Trade

Further information is available on the Department's website, or by making an enquiry to sanctions@dfat.gov.au.