Australian Government
Department of Foreign Affairs and Trade

Australian Sanctions Office

ADVISORY NOTE

INFORMATION TECHNOLOGY SECTOR

DATE: 11 June 2025

This **ADVISORY NOTE** is produced by the Australian Sanctions Office (ASO) within the Department of Foreign Affairs and Trade (DFAT). It provides a summary of a potential risk identified by the ASO 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.

INFORMATION TECHNOLOGY (IT)

The IT sector includes companies involved in the provision of products and services, including software, hardware, networking, cybersecurity, and cloud computing. Telecommunications and webhosting companies also face sanctions risks when providing services or infrastructure. **The ASO has identified that the IT sector faces heightened sanctions risks due to the following factors.**

Lower requirement to positively identify customers. The IT sector in Australia is generally not obligated to positively identify their customers. Due to this, the ASO has identified that sanctioned entities and individuals may be accessing the services and products provided by Australian IT companies. It is recommended that IT companies understand their regulatory obligations for sanctions, such as identify their customers to assess for sanctions risk. **Screening customers against the Consolidated List is the first step in sanctions compliance.**

High risk indicators include:

- Customers that are based in high-risk jurisdictions such as Iran, Russia, and the Democratic People's Republic of Korea (DPRK). Customer location may be established through language, IP address or the identification of user behaviour indicating traffic routing through proxies, and VPNs. **However, IP address must be considered in context, as they do not necessarily identify country of origin.**

- Customers who may be linked to government-related entities, politically exposed persons (PEPs), or users with links to sensitive industries (e.g., defence, oil & gas) may have heighted sanctions risk. **Links to government-related entities, PEPs, and sensitive industries may be established through registration and account details such as username and email.**

The potential for technology to service dual-purpose (civilian and military) applications. Specifically, the export of sensitive technologies or services to countries subject to sanctions can lead to significant risks. Sanctions compliance requires IT companies to conduct thorough customer risk assessments and implement robust screening processes to avoid unintentional violations. Companies should be aware of their obligations to Australian sanctions.

FURTHER INFORMATION AND RESOURCES

While this advisory 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 resources 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 - Digital Currency Exchanges | Australian Government Department of Foreign Affairs and Trade
- Guidance Note - Dealing with assets owned or controlled by designated persons and entities | Australian Government Department of Foreign Affairs and Trade.

The ASO also recommends businesses in this sector consult other official guidance. Such guidance includes information available at https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/russian-gru-targeting-western-logistics-entities-and-technology-companies.

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.