ADVISORY NOTE

Advisory Note - Democratic People's Republic of Korea (DPRK) Information Technology (IT) Workers

First Published: 26 August 2024 - Last updated: 14 December 2025

This updated advisory from the Australian Sanctions Office (ASO) alerts the community to attempts by information technology (IT) workers from the Democratic People's Republic of Korea (DPRK) to obtain remote employment, including with Australian businesses, while posing as non-DPRK nationals.

The DPRK has deployed thousands of highly skilled IT workers around the world. These IT workers seek employment in fields such as website design, graphic design, and general IT programming. The DPRK relies on IT worker operations to illicitly finance the DPRK's weapons of mass destruction and ballistic missile programs.

Payments to DPRK IT workers violate United Nations Security Council sanctions and Australia's autonomous sanctions. Employing a DPRK IT worker may constitute a serious criminal offence under Australian sanctions laws, or the sanctions laws of other countries, including the United States of America.

Advice to Australians and Australian businesses

Hiring or supporting the activities of DPRK IT workers is risky. In addition to the risk of committing a criminal offence under Australian sanctions laws, Australian businesses risk theft of intellectual property or data, improper access to personal identification details and funds, and reputational harm.

Australians and Australian businesses are encouraged to review this advisory to better understand and prevent the inadvertent hiring of DPRK IT workers.

What are the characteristics of DPRK IT workers?

DPRK IT workers deliberately obfuscate their identities, locations, and nationalities, typically using fake personas, proxy accounts, stolen identities, and falsified or forged documentation to apply for jobs. They target employers in wealthier countries, including Australia, utilising a variety of mainstream and industry-specific freelance contracting, and social media and networking platforms. In Australia, companies have been targeted through online platforms such as **Linkedin, Fiverr** and **Freelancer.**

These workers are active in a range of fields and sectors, including business, health and fitness, social networking, sports, entertainment, and lifestyle. DPRK IT workers often take on projects that involve virtual currency, or through money services businesses such as PayPal or remittance services. DPRK IT workers will also use virtual currency exchanges and trading platforms to manage digital payments they receive for contract work as well as to launder these funds back to the DPRK.

Red flag indicators of potential DPRK IT worker activity include:

- the IT worker may have a history of excessive bidding on projects, and may charge below market rates for their work;
- multiple logins into one account from various IP addresses in a relatively short period of time, especially if the IP addresses are associated with different countries;
- frequent transfers of money through payment platforms to overseas accounts - especially to the People's Republic of China (PRC), Russia, South East Asia countries, or central Asian countries such as Kazakhstan, or requests for payment in cryptocurrency;

- inconsistencies in name spelling, nationality, claimed work location, contact information, educational history, work history, and other details across a developer's freelance platform profiles, social media profiles, external portfolio websites, or payment platform profiles;
- inability to conduct business during required business hours and inability to reach the worker in a timely manner, especially through "instant" communication methods;
- the IT worker may refuse or claim they are unable to appear on camera and, if they do appear on camera, there may be inconsistencies in location or appearance; and
- the IT worker is logged into the account for excessive periods of time – for example, longer than 24 hours.

How can Australians and Australian businesses protect against DPRK IT workers?

Australians and Australian businesses can take steps to protect against the risk of employing a DPRK IT worker, such as:

- verifying all information supplied by the IT worker, including:
    - checking that the name spelling, nationality, claimed location, contact information, educational history, work history, and other details of a potential hire are consistent across the developer's freelance platform profiles, social media profiles, external portfolio websites, and payment platform accounts;
    - verifying phone numbers and being suspicious of those identified as being Voice over Internet Protocol (VoIP) numbers;
    - verifying documents submitted as part of proposal reviews or job applications directly with the listed companies and educational institutions, not utilising contact information provided on the submitted documentation;
    - closely scrutinising identity verification documents submitted for forgery;
    - conducting a video interview to assist to verify a potential freelance worker's identity;
    - conducting a pre-employment background check and/or fingerprint or biometric log-in to verify identity and claimed location;
    - conducting reverse image checks on profile images, and monitoring for the use of artificial intelligence (AI) to modify employment profile pictures;
    - being suspicious if a developer cannot receive items at the address on their identification documentation; and
    - if they have claimed previous employment from Australian companies, considering independently verifying that the company exists, and confirming employment history;
- monitor and restrict the use and installation of remote administration tools to employees you have not verified;
- require remote IT workers to shut off commercial VPNs when accessing company networks;

- avoid payments in cryptocurrency;
- require verification of banking information corresponding to other identifying documents, and be suspicious of requests for payments to be made into accounts with different names, or into different accounts; and
- consider restricting sensitive information, such as personal details of other staff, and avoid granting access to proprietary information by remote IT workers.

Compliance with Australian Sanctions Laws

If you hire a DPRK IT worker and pay them for services, you risk contravening Australian sanctions laws because you are directly or indirectly making an asset available to, or for the benefit of, a sanctioned person or entity; or because you are engaging in certain prohibited commercial activities with the DPRK.

When the ASO identifies a potential DPRK IT worker targeting an Australian business, the ASO will respond in a manner consistent with our graduated risk-based approach to compliance. While in serious cases this may result in prosecution, businesses who are trying to do the right thing usually receive education and guidance from ASO on how to comply.

As part of our communication with an affected business, the ASO may request information to determine how the DPRK IT worker was employed and other details. This communication will only occur through the sanctions@dfat.gov.au email address.

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).

For bodies corporate, it is a defence if the body corporate can prove that it took reasonable precautions and exercised due diligence to avoid the contravention. Implementing the measures outlined in this advisory may assist a body corporate to demonstrate that it took reasonable precautions and exercised due diligence.

Other Resources

For further detailed guidance on DPRK IT workers see Guidance published by the US Department of State and UK Office of Financial Sanctions Implementation (OFSI), HM treasury. For further guidance regarding Australia's sanctions in relation to the DPRK, please see our DPRK Sanctions Snapshot (dfat.gov.au).