ADVISORY NOTE

# CYBER RISKS OF DPRK IT WORKERS

**DATE: 6 November 2025**

This ADVISORY NOTE is produced by the Australian Sanctions Office (ASO) and the … 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.

The ASO has previously published an advisory on the sanctions risks 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. This advisory is focused on the cyber risks and seeks to alert the Australian community on the additional risks business maybe exposed when they inadvertently hire a DPRK IT worker.

The Democratic People's Republic of Korea (DPRK) has deployed thousands of information technology professionals for software and web development roles as part of a government revenue strategy. These skilled individuals primarily operate from locations within DPRK, China, Russia, and sometimes Southeast Asia utilising resources such as virtual private networks (VPNs) and remote monitoring and management (RMM) tools, often in collaboration with informed associates, to obscure their true locations and identities.

## Cyber risks

In recent years, there has been an increase in cyber espionage activities linked to state-sponsored actors from the DPRK, involving the use of IT workers embedded within legitimate organizations. These individuals may use their positions to access sensitive information, steal intellectual property, adversely impact organizational operations, or generate revenue that is provided back to DPRK.

Case Study: In the public "*2024 Threat Hunting Report*", CrowdStrike disclosed that they uncovered over 30 U.S.-based companies, including those in aerospace, defence, retail, and technology sectors, targeted by malicious insiders. These insiders, who posed as U.S. residents, were hired in early 2023 for remote IT positions. The report indicated that DPRK IT workers issue is prolific and high paying countries such as the U.S and Australia are specifically targeted.

## Mitigation options

The following actions can help reduce your risk of inadvertently hiring a DPRK IT worker, assist in possible detection and after care. The public advisory on DPRK IT workers provides an extensive list of indicators and mitigations strategies available on its website. These indicators listed in this advisory should be used to assess and evaluate potential risks posed by remote workers.

### Employment screening

- Australian businesses should take additional precautions when hiring a remote worker. The identity details and documentation of remote workers should be independently verified.
    - DPRK IT workers impersonate foreign or domestic teleworkers and use fraudulent tactics to bypass employment verification. They obtain or create stolen identities matching target organizations' locations, set up email and social media accounts, and build fake portfolios on platforms like GitHub and LinkedIn.

- They also use AI tools such as image generators and voice changers to support these activities. For more information on this risk, please see (insert hyperlink to the Misuse of AI advisory)

### Ongoing monitoring and risk mitigation options

- Australian businesses should be aware of the potential indicators of remote DPRK IT workers, and continue to assess their remote staff for high-risk behaviour.
- Consideration should be given to the breadth of access remote workers have to systems – particularly sensitive data including payroll and personal information.
- Business should consider auditing access logs to determine if remote workers have accessed material non-essential to their role.
- IT Security sweeps should be conducted regularly to identify unauthorised new software and malicious code that may have been introduced into products.

### Post detection requirements

- If you have detected or hold suspicions that a remote worker may be a DPRK IT worker, please contact Australian Sanctions Office and suspend all future payments until further direction. Further payments may be viewed as sanctions contraventions.
- The suspected worker should have their remote access limited or removed until their identity is confirmed.
- Evaluate the potential risk your business may be exposed to based off the remote workers access and their role.
- Conduct through IT security screening if your network to determine what material has been accessed, and if any authorised software has been uploaded, or malicious code has been inserted into existing programs.

**Case Study:** A public example of an incidents involving DPRK IT Worker include "*KnowBe4*[1]," a cybersecurity training company. This case illustrates changing methods used by DPRK-related cyber actors and emphasize the importance of strong security protocols and careful hiring procedures across various industries.

## 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
- Office of Public Affairs | Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes | United States Department of Justice
- DPRK IT WORKERS — FBI

[1] How a North Korean Fake IT Worker Tried to Infiltrate Us

The US Department of Justice and the Federal Bureau of Investigations regularly provides information to the public on known DPRK IT worker profiles.

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