ADVISORY ON DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (DPRK) INFORMATION TECHNOLOGY (IT) WORKERS

The Australian Sanctions Office, in the Department of Foreign Affairs and Trade, is publishing an advisory to alert the community to attempts by the Democratic People's Republic of Korea (DPRK) and remote DPRK information technology (IT) workers to obtain employment while posing as non-DPRK nationals.

The DPRK has dispatched thousands of highly skilled IT workers around the world. The DPRK extensive illicit IT worker operations help finance the regime's unlawful weapons of mass destruction and ballistic missile program. DPRK IT workers earn revenue for the DPRK that contributes to its weapons programs in violation of United Nations Sanctions Committee and Australia's autonomous sanctions.

Advice to Australians and Australian businesses

Hiring or supporting the activities of DPRK IT workers poses many risks, ranging from theft of intellectual property, data, and funds to reputational harm. You may also face legal consequences under Australia's sanctions framework or by authorities in other jurisdictions such as the United States of America.

This advisory provides information to the public to better understand and prevent against inadvertent hiring of DPRK IT workers.

Illicit worker IT revenue generation

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 located in wealthier countries (including Australia), utilising a variety of mainstream and industry-specific freelance contracting, and social media and networking platforms.

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. DPRK IT workers also use virtual currency exchanges and trading platforms to manage digital payments they receive for contract work as well as to launder these illicitly obtained funds back to the DPRK.

Some red flag indicators of potential DPRK IT worker activity include:

- 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, especially to People's Republic of China (PRC)-based bank accounts, 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, payment platform profiles, and assessed location and hours; and
- Inability to conduct business during required business hours and inability to reach the worker in a timely manner, especially through "instant" communication methods.

What does this mean for Australians and Australian businesses? Here's what you need to do:

- Verify 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 scrutinise identity verification documents submitted for forgery;
- Conduct a video interview to verify a potential freelance worker's identity;
- Conduct a pre-employment background check and/or fingerprint/biometric log-in to verify identity and claimed location;
- Avoid payments in cryptocurrency and require verification of banking information corresponding to other identifying documents;
- Check 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, payment platform accounts, and assessed location and hours of work; and
- Be suspicious if a developer cannot receive items at the address on their identification documentation.

Compliance with Australian Sanctions Laws

By hiring a DPRK IT worker and paying them for services, there is a risk that you might directly or indirectly breach sanctions prohibitions against making assets available to, or for the benefit of, a sanctioned person or entity. There are also risks related to engaging in certain commercial activities with the DPRK.

Remember, Australian sanction laws apply broadly, including to activities:

- in Australia;
- by Australian citizens and Australian-registered bodies corporate overseas; and
- on board Australian-flagged vessels and aircraft.

Offences

Australian sanction laws establish serious criminal offences for contravening a sanctions measure or a condition of a sanctions permit. These offences are punishable for individuals by up to 10 years in prison, and/or a fine the greater of 2500 penalty units ($782,500) or three times the value of the transaction.

They are punishable for bodies corporate by a fine the greater of 10,000 penalty units ($3.13 million) or three times the value of the transaction. These 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.

False or misleading information

Australian sanction laws establish serious criminal offences for giving false or misleading information in connection with the administration of a sanction law.

These offences are punishable by up to 10 years in prison and/or a fine of 2500 penalty units ($782,500).

A sanctions permit is taken never to have been granted if false or misleading information was contained in the application for the permit.

Other Resources

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