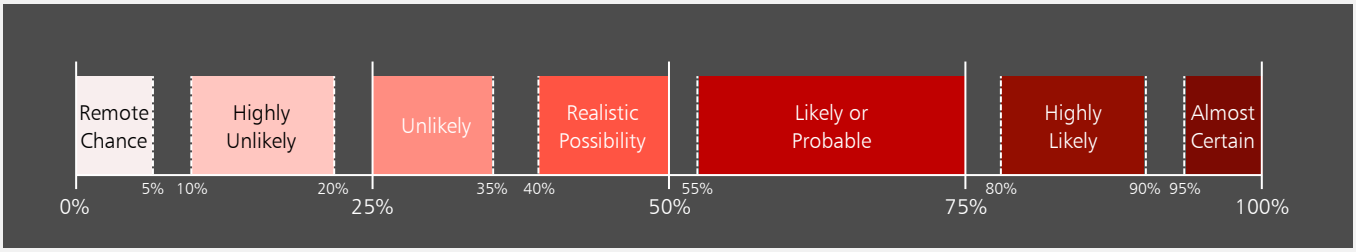
Advisory on North Korean IT Workers

KEY THREATS

1. It is **almost certain** that UK firms are currently being targeted by Democratic People's Republic of Korea (DPRK a.k.a. North Korea) Information Technology (IT) workers disguised as freelance third-country IT workers to generate revenue for the DPRK regime.
2. It is **highly likely** that DPRK IT workers are presently using online freelance platforms or job marketplaces to advertise their services to secure employment with UK firms.
3. It is **highly likely** that DPRK IT workers are using both witting and unwitting enablers, including aliases, false or fraudulent personae and proxies, to mask their true identities and hide links to the DPRK.
4. It is **likely** that DPRK IT workers make use of Virtual Private Network (VPN), Virtual Private Server (VPS) or other proxy services, such as remote desktop applications, to obscure their true locations.
5. It is **highly likely** that DPRK IT workers are leveraging alternative payment methods, such as those offered by electronic money institutions (EMIs), money service businesses (MSBs) and cryptoasset exchange providers to secure funds earned through their illicit employment.
6. DPRK IT workers may gain privileged access to sensitive or critical company information. There is a **realistic possibility** that this could result in this information being compromised or misused by other malign DPRK cyber actors.

Probability Yardstick

This advisory uses probabilistic language as detailed in the Probability Yardstick developed by HMG's Professional Head of Intelligence Assessment (PHIA).



Introduction

HM Treasury's Office of Financial Sanctions Implementation (OFSI) is the UK's competent authority for the implementation of financial sanctions. OFSI is issuing this advisory to stakeholders, including the private sector, to highlight threats to compliance with UK and United Nations (UN) sanctions relating to the Democratic People's Republic of Korea (DPRK, a.k.a. North Korea); namely, DPRK information technology (IT) workers fraudulently gaining employment with companies in the UK, US and elsewhere to raise revenue for the DPRK regime. This advisory provides detailed information on DPRK IT workers as well as associated red flags and mitigations to assist stakeholders in better understanding and protecting against this threat. This advisory does not represent legal advice and should be read in conjunction with general guidance on the UK's sanctions in relation to the DPRK.

Compliance with UK Financial Sanctions

The DPRK is subject to significant sanctions measures imposed by the UK in accordance with its obligations under UN Security Council resolutions. They are aimed at countering the proliferation of weapons of mass destruction (WMD) and ballistic missiles. As outlined below, individuals and entities who employ or pay DPRK IT workers could be directly or indirectly breaching financial sanctions.

There are both civil and criminal enforcement options to remedy breaches of financial sanctions. Civil monetary penalties can be applied to persons for breaches of financial sanctions legislation with no requirement for OFSI to demonstrate that the person knew or had reasonable cause to suspect the conduct amounted to a breach of sanctions. A breach of financial sanctions may also be a criminal offence, punishable upon conviction by up to 7 years in prison.

Reporting

OFSI encourages all stakeholders to report to OFSI if you suspect you or others are being targeted by DPRK IT workers or are otherwise affected by the threats outlined in this advisory. Further information about obligations to report to OFSI can be found in chapter 5 of our UK financial sanctions general guidance. Further instructions on how to report suspected breaches of financial sanctions to OFSI are available here.

Suspicious Activity Reports (SARs)

If you know or suspect that there has been money laundering or terrorist financing activity and your business falls within the regulated sector, then you are reminded of the obligations to make reports to the National Crime Agency (NCA) under Part 7 of the Proceeds of Crime Act 2002 and the Terrorism Act 2000. If you decide to make a report in this way you should adopt the usual mechanism for doing so, and it will help analysis if you would include the reference OFSI – DPRK IT Workers Advisory – 0924 within the text should you identify activity which may be indicative of any of the typologies detailed in this report. Guidance on SARs is available here.

Nature of the Threat

The DPRK deploys highly skilled IT workers abroad to fraudulently gain employment with companies in the UK, US and elsewhere, and raise revenue for the DPRK regime.

These workers primarily operate from Russia and China, but also other parts of Asia, Africa and Latin America. They often pose as remote, non-DPRK nationals to secure freelance contracts and use a variety of techniques to mask links to the DPRK, including false representation of identity, nationality and location, and the use of non-DPRK enablers, who provide services that enable DPRK IT workers to conduct their activities.

DPRK IT workers have skills in areas including, but not limited to, software development, IT support, graphic design, and animation.

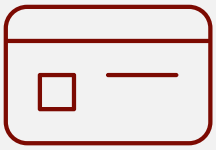
Delegations of DPRK IT workers operate through complex networks of companies and individuals on behalf of the DPRK Government, including the Munitions Industry Department, the Ministry of Atomic Energy Industry, and the Ministry of National Defence, all designated under the UK's Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019 for their involvement in key aspects of the DPRK's banned WMD, ballistic missile and military programmes. Revenue funds obtained by DPRK IT workers are used to purchase UN-prohibited goods and military equipment. This revenue also contributes to the DPRK's illicit WMD and missile programmes.

Proliferation financing of this kind more broadly threatens the stability of the UK and global financial system and poses a clear international security risk. The UK will continue to take proactive steps to tackle proliferation financing and publicise trends and typologies proliferating actors – such as the DPRK – undertake to finance their chemical, biological, radiological and nuclear weapons programmes.

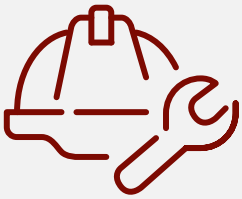
A DPRK worker can earn substantial amounts, often by maintaining multiple long term and full-time positions while simultaneously conducting freelance work.

Affected UK Sectors

Information Technology (IT)



Electronic Money Institution (EMI)/ Money Service Business (MSB)



Professional Services

Cryptocurrency

How DPRK IT Workers Operate

The following section outlines common practices used by DPRK IT workers when soliciting work with UK firms, as well as associated **red flags**. While the red flags do not signify illicit activity in and of themselves, they could be indicative of DPRK IT worker activity, especially when two or more are present, and should trigger increased due diligence.

Target UK industry

- DPRK IT workers provide prospective employers with false curriculum vitaes (CVs) to secure employment.
- Successful job procurement then results in recommending other DPRK IT workers to obtain positions at the same company.

- Inconsistent or changing: name spelling; nationality; location; contact information; education or work history; and online presence.
- Failure to complete project tasks.
- Refusal to appear on camera, conduct video interviews or meetings (favouring text-based chat).
- Request prepayment but do not meet project benchmarks or attend check-in meetings.
- At first offer to provide free services to earn trust, seeking long term contracts.
- Claim previous employment with UK firms to solicit employment.

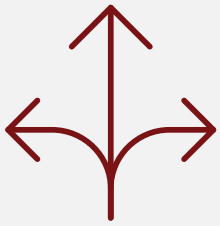
Use of online platforms

- Advertise IT services via online platforms for freelance work or job marketplaces.
- Use of software development tools and platforms, messaging applications, and social media and networking websites to find roles.
- Use of an intermediary firm for talent acquisition/recruitment to help the IT worker secure employment.

- Multiple logins into one account from various IP addresses in a short period of time.
- Logins into multiple accounts on the same platform from a single IP address.
- Logged into account continuously for 1+ days.
- Multiple accounts using the same templates.
- Multiple accounts receive high ratings from one client account in a short period of time.
- Extensive bidding on projects but low acceptance rate.
- Use of platform account resale services.

Use of witting enablers

- Non-DPRK nationals rent out their identities for profit in order to:
  - Provide DPRK IT workers with accounts using false identities or aliases to circumvent identity verification.
  - Complete email, phone and ID verification on behalf of the DPRK IT worker.
  - Attend interviews or meetings with employers/clients on behalf of the DPRK IT worker.
- They also:
  - Provide infrastructure services, such as laptops or desktops, which are accessed remotely to obscure DPRK IT workers' true location.
  - Use front companies to hide links to the DPRK.



- Biographical information does not match the applicant.
- Inconsistencies when they appear on camera (time, location or appearance).
- Indications of cheating on coding tests or when conducting interviews.
- Online presence does not match the hired IT worker's CV.
- Multiple online profiles with different pictures, or online profiles with no picture.

Use of unwitting enablers

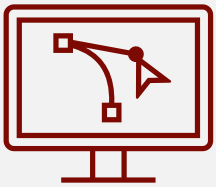
DPRK IT workers may:

- Solicit non-DPRK residents for job procurement platform accounts.
- Advertise on freelance platforms using false non-DPRK personae or aliases.
- Use multiple non-DPRK identities simultaneously.
- Use false and/or fraudulent documents.
- Use faceswap applications.
- Steal customer account information to verify identities with freelance platforms, payment providers and employers.

- Propose collaboration on development projects with non-DPRK freelancers.
- Ask co-workers to borrow personal information to obtain other contracts.
- Request to borrow proxy accounts via social media.
- Claim to be experienced an IT worker from third countries seeking higher hourly rates for freelance work.
- Use of anglicised names or pseudonyms.
- Offer to pay non-DPRK residents a fee for use of their proxy account, sometimes more if the resident has prior experience in the field and/or is willing to conduct calls with clients.
- Request individuals with a native or high level of English to conduct video and phone interviews with prospective employers and/or clients on their behalf.
- Ask to be contacted directly via social media or messaging applications.

Use of VPN/VPS/proxy services

- Use of Virtual Private Server (VPS), Virtual Private Network (VPN) or proxy services to obscure location.
- Use of remote desktop applications.
- Use of laptop farms to remotely access computers or laptops in friendly jurisdictions (the IP address for the laptop will be that of the laptop farm).



- Prefer remote working arrangements.
- Use a single, dedicated device for each account.
- Technical configurations linked with use of remote desktop sharing software.
- Request hardware to be sent to an address not listed on the IT worker's ID documentation.
- Claim to not be able to receive items at the address on ID documentation.
- Operate outside declared business hours.
- Not reachable in a timely manner.

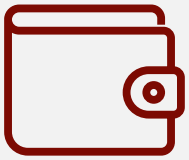
Use of Electronic Money Institutions (EMIs)/ Money Service Businesses (MSBs)

- Purchase EMI or MSB accounts via third parties.
- Pay non-DPRK residents for use of their proxy accounts via EMI/MSB.
- Funds earned deposited directly to the DPRK IT worker's EMI/MSB accounts.
- Use enablers to consolidate their earnings into bank accounts in the enablers' name.

- Request to be paid into an account using someone else's name.
- IT worker's bank account is blocked/ deactivated or not accepting payment.
- IT worker needs to switch bank account.
- Different individuals (e.g., both client and IT worker) use the same EMI account to transfer/withdraw money.
- Different EMI/MSB customers share the same device.
- Frequent transfers of funds through payment platforms.
- EMI/MSB customers receive funds from and deposit them to each other.
- Payments made to China-based bank accounts.

Use of cryptocurrencies

- Use virtual currency exchanges and trading platforms to manage digital payments and launder funds.
- Move cryptocurrencies between accounts.
- May establish new cryptocurrency trading platforms.



- Request to be paid in cryptocurrency.
- Seek web3, blockchain, smart contracts and cryptocurrency projects in community chat rooms, forums, social media or freelance platforms.

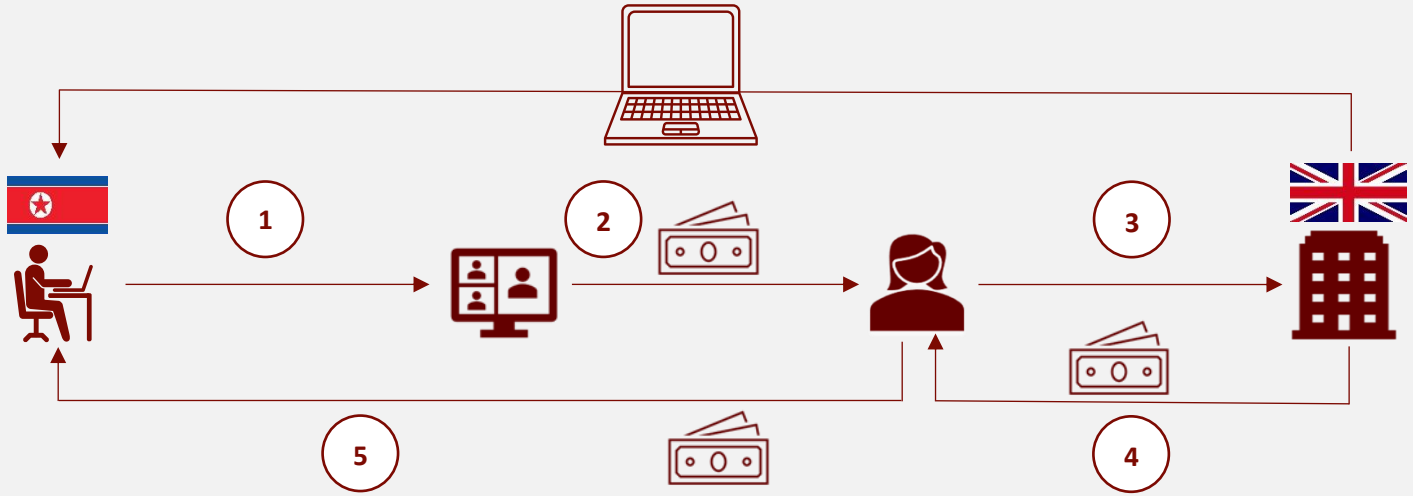
Privileged access

- Collaborate with or support other DPRK cyber actors.
- Exploit and/or build vulnerabilities into smart contracts to steal funds.
- Carry out small scale cryptocurrency thefts or other financially motivated criminality.
- Infiltrate company networks to maintain access for hacking and extortion schemes.

- Threaten to release proprietary source codes if payments are not made.
- Participate in white hat competitions and bug bounty programmes to identify vulnerabilities.

CASE STUDY 1: DPRK IT Worker Job Procurement Process

The UK company unknowingly interacts with and provides revenue to a DPRK IT worker.

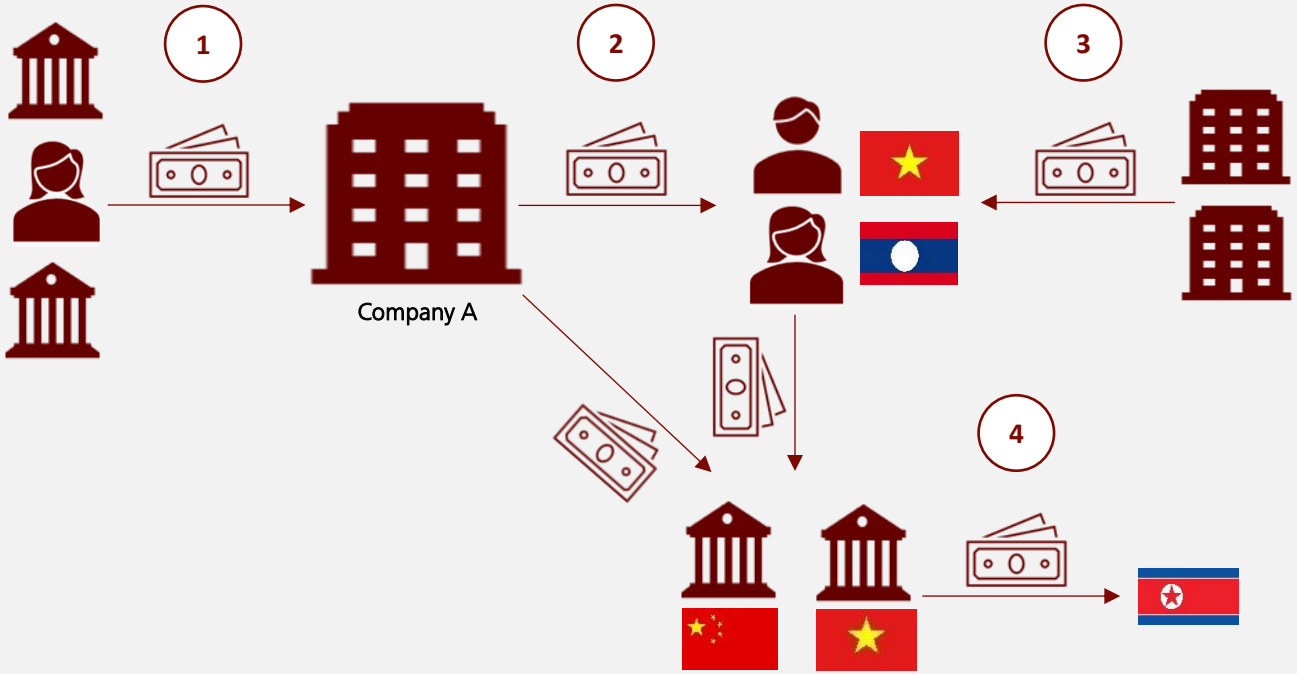


1. A DPRK IT worker advertises services on an online platform using a false non-DPRK identity.
2. A non-DPRK resident agrees to act as a proxy for the IT worker in exchange for a fee, not suspecting the IT worker's real identity.
3. The unwitting enabler secures a freelance contract with a UK IT client.
4. The client unknowingly provides hardware to the DPRK IT worker at an uncorroborated address, and processes payment to the enabler's EMI account.
5. The enabler keeps a share of the profit and transfers the rest back to the DPRK IT worker's bank account.

- Uses false name or alias.
- Offers to pay residents a fee to set up and/or verify their account.
- Requests individuals with high levels of English to conduct video and phone interviews with prospective employers.
- Provides payment directly to the resident via Electronic Money Institution (EMI) or Money Service Business (MSB).
- Asks to be contacted directly via social media or messaging applications.

CASE STUDY 2: DPRK IT Workers' Use of Front Companies and Electronic Money Institutions (EMIs)

Company A operates as a front company to obtain funds for the DPRK.



1. An IT company, Company A, receives large deposits to its UK EMI account from business and personal bank accounts and a significant sum from its own bank account.
2. The funds are transferred to individual accounts from Vietnam and Laos within the same EMI, and to bank accounts in China and Vietnam.
3. The individuals also receive funds from various other IT companies.
4. The received funds are then transferred out to personal bank accounts in China and Vietnam, and then ultimately to the DPRK.

- Links to foreign jurisdictions with known ties to the DPRK.
- Frequent third-party deposits.
- EMI customers receive funds from and deposit them to each other.
- EMI customers share the same device.
- Use of non-DPRK financial enablers.

Mitigations

Below are some potential mitigation measures for UK firms to protect themselves against hiring or facilitating the operations of DPRK IT workers[1].

UK firms hiring IT workers:

- Use reputable online freelance platforms that offer robust verification measures of IT workers.
- Be vigilant against requests to communicate outside the original freelance platform website.
- Conduct video interviews.
- Ensure IT worker's information is consistent across profiles (freelance platforms, social media, external websites, payment platforms) and declared location and working hours.
- Conduct preemployment background checks.
- Check identity verification documents for forgery.
- Verify contact information provided by IT worker.
- Verify employment and higher education history.
- Require freelancers to shut off commercial VPNs when accessing company networks.
- Consider disabling remote collaboration applications on computers supplied to freelance IT workers.
- Monitor the IP addresses of remote IT workers.
- Use extra caution when interacting with freelance developers through remote collaboration applications.
- Flag IT workers who cannot receive equipment at address listed on their identification documents.
- Avoid payments in cryptocurrency.
- Limit access in accordance with Zero Trust and Need-to-Know policies.
- Avoid granting access to proprietary information.
- Avoid recruiting freelance workers directly through online IT competitions.
- Be vigilant for unauthorised, small-scale transactions.

[1]UK businesses should continue to ensure they comply with their legal obligations, including date protection legislation.

Freelance work platform companies:

- Require video verification.
- Reject low-quality verification images.
- Provide extra scrutiny to newly established accounts.
- Verify the existence of any websites provided to establish accounts.
- Flag accounts with high numbers of project bids but low-bid acceptance rates, or low numbers of account logins.
- Flag accounts using the same/similar documentation.
- Flag accounts receiving high ratings from a single client account in a short of time.
- Deny activity in newly established accounts prior to full account verification.
- Flag accounts that use the same digital payment service accounts. period
- Use port checking utilities to determine if the platform is being accessed remotely via desktop sharing software, VPN or VPS.

Electronic Money Institutions (EMIs) / Money Service Businesses (MSBs):

- Require verification of banking information in line with other identifying documents.
- Be vigilant against frequent transfers of funds to or from China-based bank accounts.
- Be vigilant against funds routed through one or more companies to disguise their ultimate destination.
- Flag customers that share the same device for multiple accounts.
- Flag accounts that use similar or identical documentation.
- Flag accounts that frequently receive funds from or deposit them to each other.

Other Resources

For further detailed guidance on DPRK IT workers see guidance published by the U.S. Department of the Treasury Office of Foreign Assets Control, and for general guidance on the UK's sanctions in relation to the DPRK, please see Democratic People's Republic of Korea sanctions: guidance - GOV.UK (www.gov.uk). For more information and guidance on UK financial sanctions, visit the OFSI homepage.

Office of Financial
Sanctions Implementation
HM Treasury