FACT SHEET:

GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS

May 16, 2022

The U.S. Government is issuing this **advisory** as a comprehensive resource for the international community, the private sector, and the public to better understand and guard against inadvertent recruitment, hiring, and facilitation of Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) information technology (IT) workers. The advisory provides detailed information on how DPRK IT workers operate and identifies red flag indicators and due diligence measures to help companies avoid hiring DPRK freelance developers and to help freelance and digital payment platforms identify DPRK IT workers abusing their services. Hiring or supporting the activities of DPRK IT workers poses many risks, ranging from theft of intellectual property, data, and funds to reputational harm and legal consequences, including sanctions under both U.S. and United Nations (UN) authorities.

The DPRK has dispatched thousands of highly skilled IT workers around the world, earning revenue for the DPRK that contributes to its weapons programs in violation of U.S. and UN sanctions. These workers:

- Abuse the entire ecosystem of freelance work platforms to surreptitiously obtain IT development contracts from client companies around the world—as well as abuse many social media platforms—to communicate with clients and payment platforms to receive payment for their work;
- Develop applications and software spanning a range of sectors, including, but not limited to, business, cryptocurrency, health and fitness, social networking, sports, entertainment, and lifestyle;
- In many cases misrepresent themselves as foreign (non-North Korean) or U.S.-based teleworkers, including by using virtual private networks (VPNs), virtual private servers (VPSs), purchased third-country IP addresses, proxy accounts, and falsified or stolen identification documents; and
- Use privileged access gained as contractors for illicit purposes, including enabling malicious cyber intrusions by other DPRK actors.

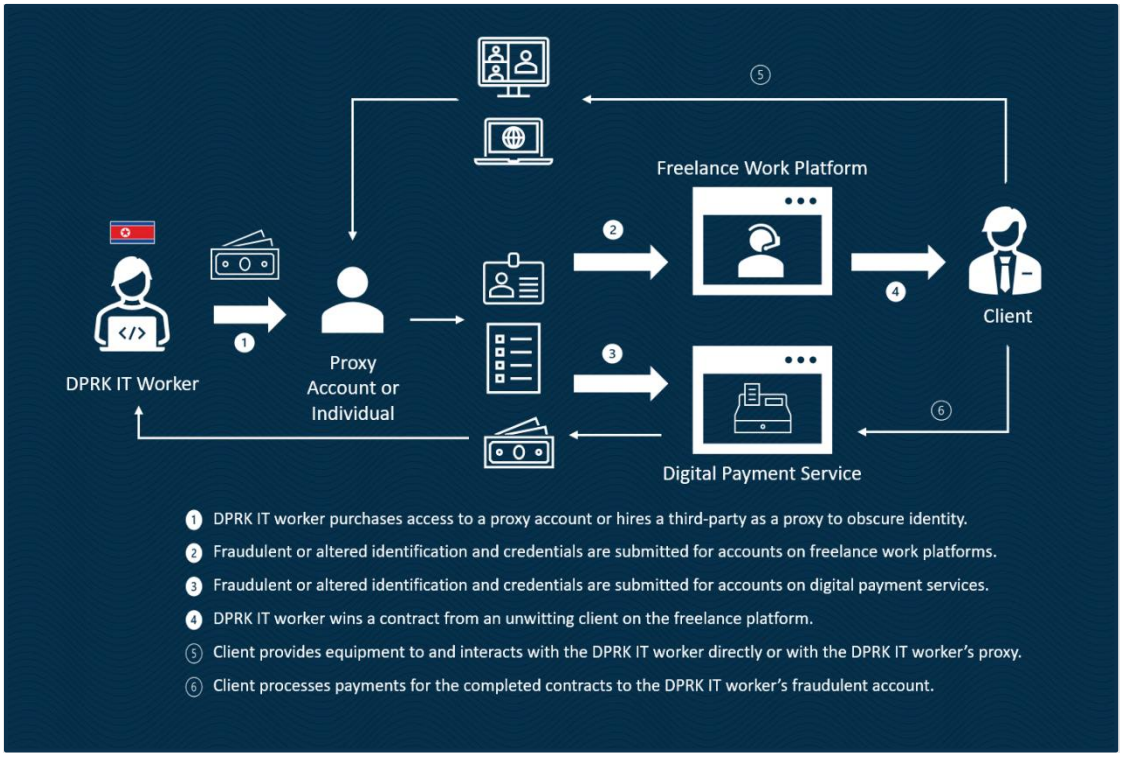
Some red flag indicators of potential DPRK IT worker activity include:

- 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.

Due diligence measures the private sector can consider to prevent inadvertent or unwitting hiring of DPRK IT workers include:

- Verify documents submitted as part of proposal reviews or job applications directly with the listed companies and educational institutions (not utilizing contact information provided on the submitted documentation);
- Closely scrutinize 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.

Overview of DPRK IT Worker Operations



*For more information, please see the **DPRK Cyber Advisory**, visit the **Treasury resource center**, and/or contact your **local FBI office**. If you have information about illicit DPRK activities in cyberspace, including past or ongoing operations, you could be eligible to receive an award of up to $5 million by providing such information through the Department of State's **Rewards for Justice** program.*