Kingdom of Cambodia

Nation Religion King

COMMERCIAL GAMBLING MANAGEMENT COMMISSION OF CAMBODIA
GENERAL SECRETARIAT

Presentation

on

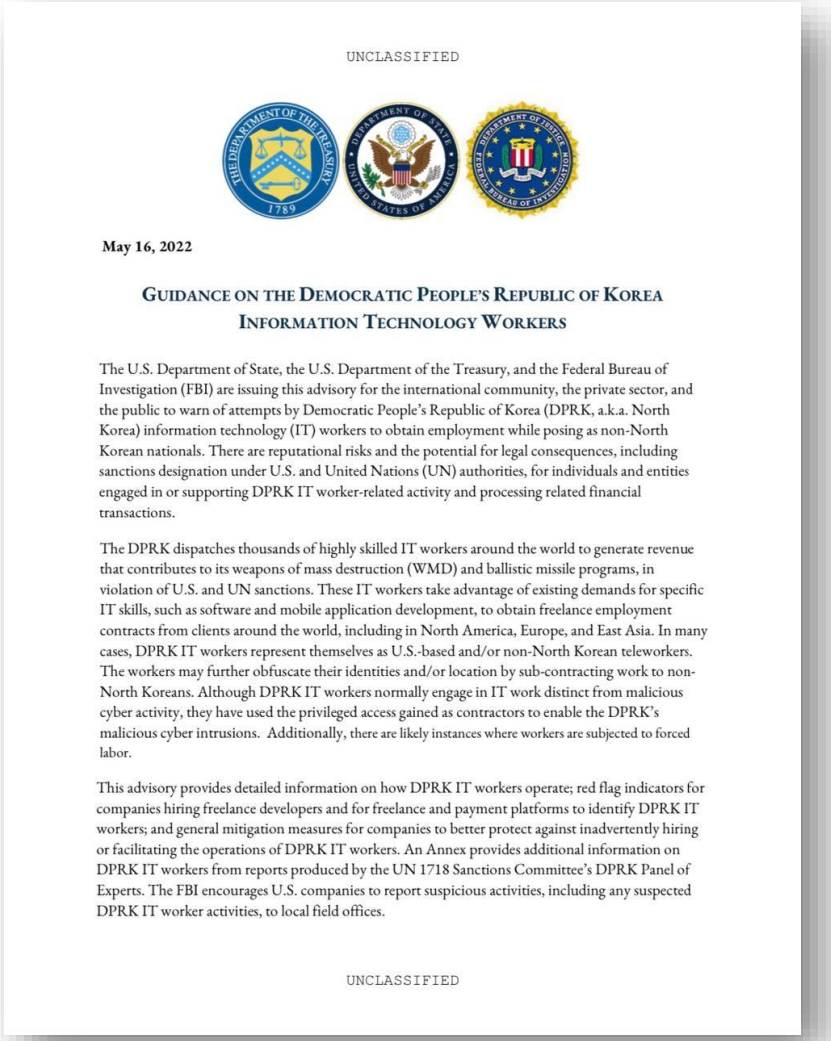
DPRK IT WORKERS – Risks, Red Flags and Recommendations

Prepared by: AML/CFT Working Group of General Secretariat of **CGMC**

2024

Content

1 - Origin of Advisory



UNCLASSIFIED

May 16, 2022

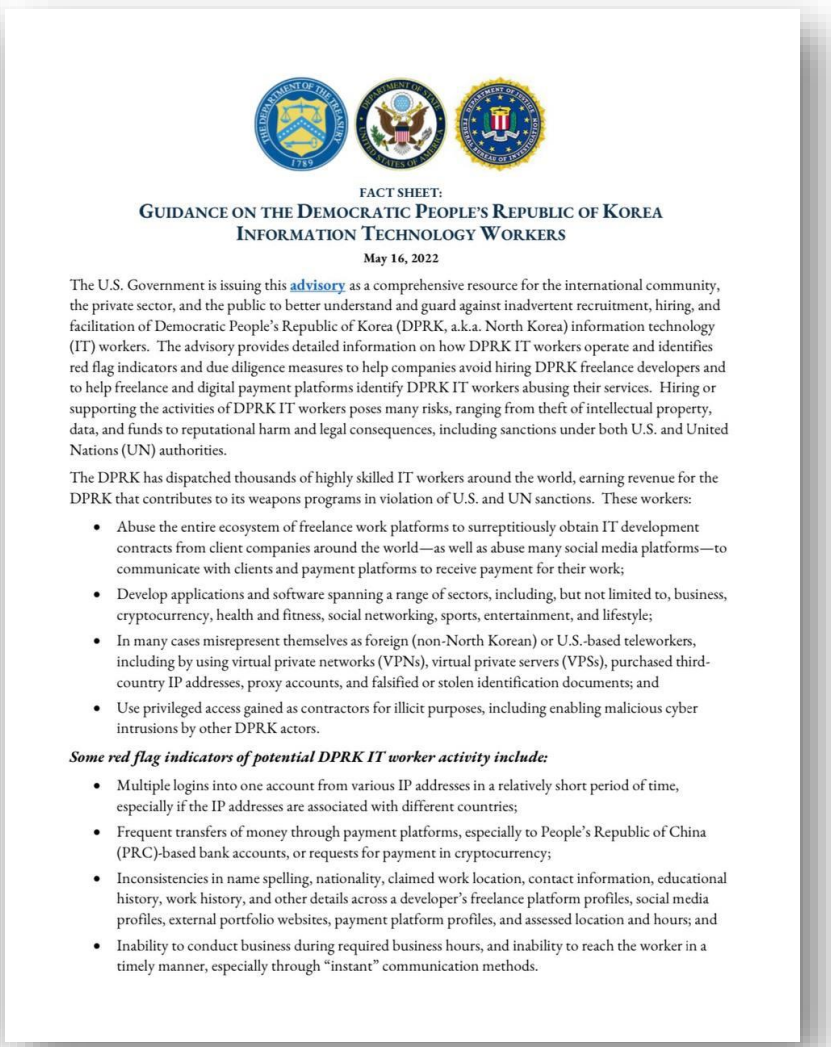
GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS

The U.S. Department of State, the U.S. Department of the Treasury, and the Federal Bureau of Investigation (FBI) are issuing this advisory for the international community, the private sector, and the public to warn of attempts by Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) information technology (IT) workers to obtain employment while posing as non-North Korean nationals. There are reputational risks and the potential for legal consequences, including sanctions designation under U.S. and United Nations (UN) authorities, for individuals and entities engaged in or supporting DPRK IT worker-related activity and processing related financial transactions.

The DPRK dispatches thousands of highly skilled IT workers around the world to generate revenue that contributes to its weapons of mass destruction (WMD) and ballistic missile programs, in violation of U.S. and UN sanctions. These IT workers take advantage of existing demands for specific IT skills, such as software and mobile application development, to obtain freelance employment contracts from clients around the world, including in North America, Europe, and East Asia. In many cases, DPRK IT workers represent themselves as U.S.-based and/or non-North Korean teleworkers. The workers may further obfuscate their identities and/or location by sub-contracting work to non-North Koreans. Although DPRK IT workers normally engage in IT work distinct from malicious cyber activity, they have used the privileged access gained as contractors to enable the DPRK's malicious cyber intrusions. Additionally, there are likely instances where workers are subjected to forced labor.

This advisory provides detailed information on how DPRK IT workers operate; red flag indicators for companies hiring freelance developers and for freelance and payment platforms to identify DPRK IT workers; and general mitigation measures for companies to better protect against inadvertently hiring or facilitating the operations of DPRK IT workers. An Annex provides additional information on DPRK IT workers from reports produced by the UN 1718 Sanctions Committee's DPRK Panel of Experts. The FBI encourages U.S. companies to report suspicious activities, including any suspected DPRK IT worker activities, to local field offices.

UNCLASSIFIED



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.

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 (North Korea) information technology (IT) workers. As 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.

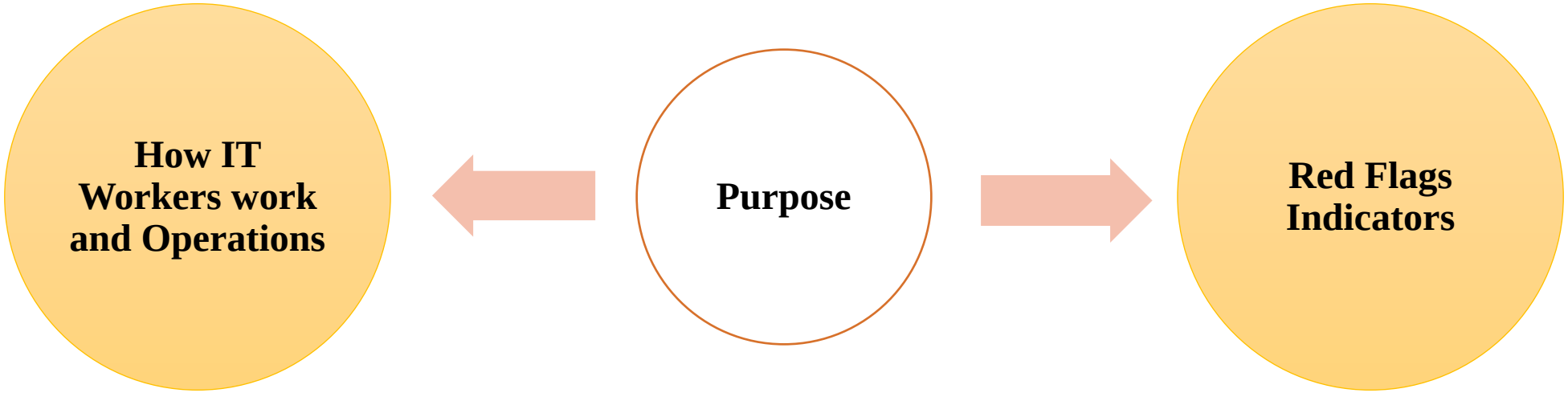
1 - Origin of Advisory (Cont.)

The Panel first reported on DPRK IT workers in its 2019 Midterm Report, noting that the MID was using its subordinate trading corporations to station abroad DPRK information technology workers, such as software programmers and developers, in order to earn foreign currency.

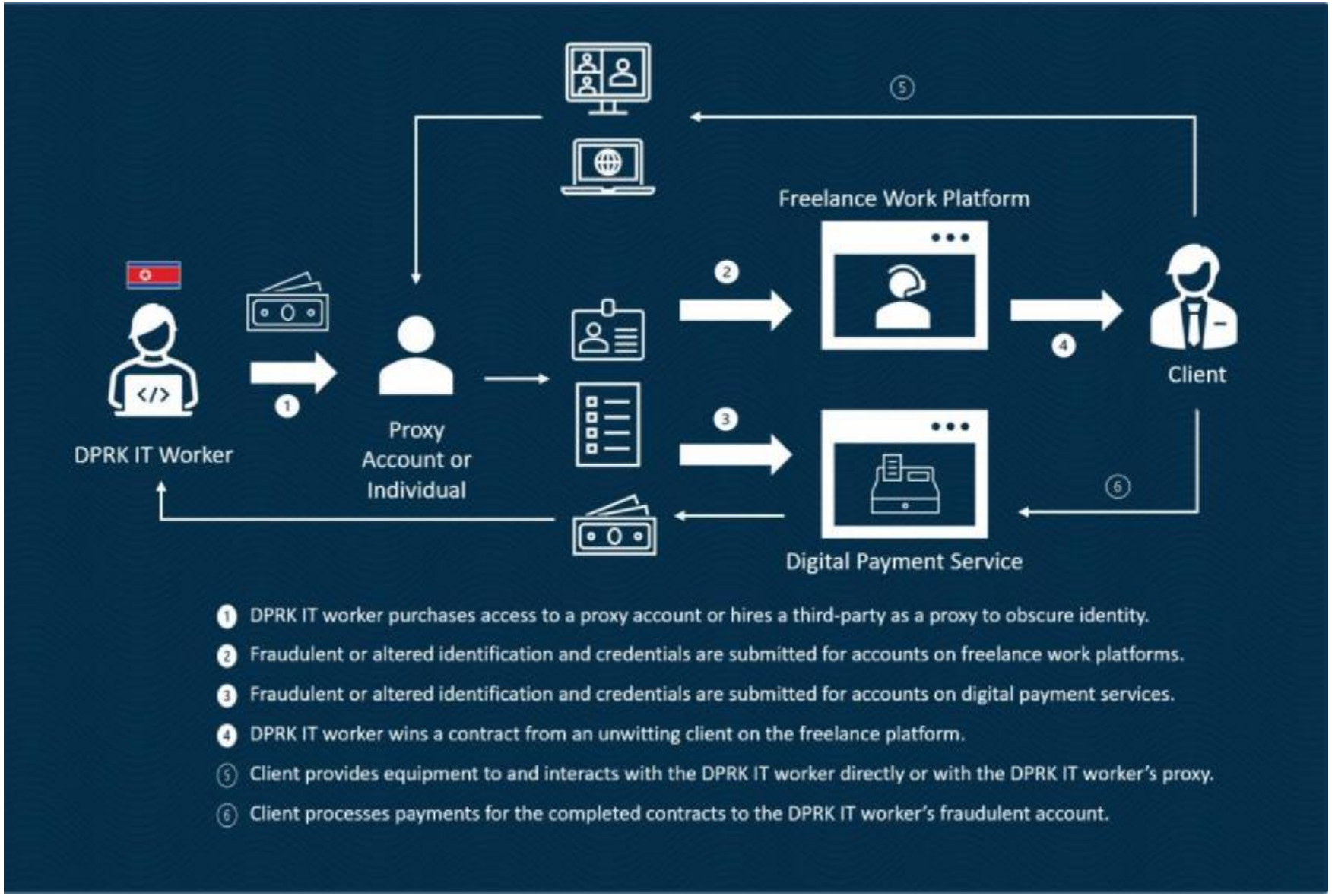
Most overseas DPRK IT workers are employed by companies subordinate to MID, suspected of having dispatched at least 1,000 IT workers overseas for the purpose of revenue generation, often using subordinate entities or front companies.

DPRK IT workers can evade employers' due diligence efforts and KYC/AML protocols by employing similar obfuscation methods as those utilized by the DPRK to access the international financial system, including providing false identification, use of VPN services, and establishing front companies.

2 - Purpose of Advisory



3 - Operations of DPRK IT workers



3 - Operations of DPRK IT workers (Cont.)

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 freelance work platforms by obtain IT development contracts from client companies around the world—to communicate with clients and payment platforms to receive payment for their work;
- Develop applications and software spanning a range of sectors, including, business, cryptocurrency, health and fitness, social networking, sports, entertainment, and lifestyle;
- Misrepresent themselves as foreign (non-North Korean) or U.S.-based teleworkers, 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

3 - Operations of DPRK IT workers (Cont.)

DPRK IT companies and their workers engage: (1). mobile applications and web-based applications, (2).Build computer Anti-Virus Program (3). building virtual currency exchange platforms and digital coins, (4). online gambling programs, (5). mobile games.

4 - Red Flag Indicators

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

1. Multiple logins into one account from various IP addresses in a relatively short period of time
2. Frequent transfers of money through payment platforms, especially to People's Republic of China (PRC)-based bank accounts, or requests for payment in cryptocurrency;
3. 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
4. Inability to conduct business during required business hours, and inability to reach the worker in a timely manner, especially through "instant" communication methods

5 - Consequences and Sanction

1. UN Security Council resolutions 2321, 2371, and 2397 highlight that the revenue generated from overseas DPRK workers contributes to the DPRK's nuclear weapons and ballistic missile programs.

2. The Department of the Treasury's Office of Foreign Assets Control (OFAC) has the authority to impose financial sanctions on any person determined to have, among other things:

- Engaged in significant activities on behalf of the Government of the DPRK or the Workers' Party
- Sold, supplied, transferred, or purchased, directly or indirectly, to or from the DPRK
- Materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support

Thank you!