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.

DPRK IT WORKERS: BACKGROUND

DPRK IT workers provide a critical stream of revenue that helps fund the DPRK regime's highest economic and security priorities, such as its weapons development program. DPRK leader Kim Jong Un recognizes the importance of IT workers as a significant source of foreign currency and revenue and supports their operations.

There are thousands of DPRK IT workers both dispatched overseas and located within the DPRK, generating revenue that is remitted back to the North Korean government. DPRK IT workers are located primarily in the People's Republic of China (PRC) and Russia, with a smaller number in Africa and Southeast Asia. These IT workers often rely on their overseas contacts to obtain freelance jobs for them and to interface more directly with customers.

All DPRK IT workers earn money to support North Korean leader Kim Jong Un's regime. The vast majority of them are subordinate to and working on behalf of entities directly involved in the DPRK's UN-prohibited WMD and ballistic missile programs, as well as its advanced conventional weapons development and trade sectors. This results in revenue generated by these DPRK IT workers being used by the DPRK to develop its WMD and ballistic programs, in violation of U.S. and UN sanctions. Many of these entities have been designated for sanctions by the UN and United States. DPRK entities dispatching DPRK IT workers include:

- **The 313 General Bureau of the Munitions Industry Department (MID)**, which controls the DPRK's research and development and productions of weapons—to include nuclear weapons and ballistic missiles—and other military equipment. The MID is subordinate to the Korean Worker's Party Central Committee and, through the 313 General Bureau, deploys a majority of the DPRK's IT work force overseas. All property and interests in property of the Workers' Party of Korea is blocked pursuant to Executive Order (E.O.) 13722.

- **The Ministry of Atomic Energy Industry**—a critical player in the DPRK's development of nuclear weapons and in charge of day-to-day operation of the DPRK's nuclear weapons program. The Ministry of Atomic Energy Industry is designated pursuant to E.O. 13382.

- Military entities subordinate to the **Ministry of Defense and Korea People's Army**. The Korean People's Army is designated on the Specially Designated Nationals and Blocked Property List.

- Lesser-known entities, such as the **DPRK Education Commission's Foreign Trade Office** and the **Pyongyang Information Technology Bureau of the Central Committee's Science and Education Department**. All property and interests in property of the Government of the DPRK is blocked pursuant to E.O. 13722.

An overseas DPRK IT worker earns at least ten times more than a conventional North Korean laborer working in a factory or on a construction project overseas. DPRK IT workers can individually earn

more than USD 300,000 a year in some cases, and teams of IT workers can collectively earn more than USD 3 million annually. A significant percentage of their gross earnings supports DPRK regime priorities, including its WMD program.

DPRK IT companies and their workers normally engage in a wide range of IT development work of varying complexity and difficulty, such as:

- mobile applications and web-based applications,
- building virtual currency exchange platforms and digital coins,
- general IT support,
- graphic animation,
- online gambling programs,
- mobile games,
- dating applications,
- artificial intelligence-related applications,
- hardware and firmware development,
- virtual reality and augmented reality programing,
- facial and biometric recognition software, and
- database development and management.

Applications and software developed by DPRK IT workers span 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. Some DPRK IT workers have designed virtual currency exchanges or created analytic tools and applications for virtual currency traders and marketed their products themselves.

For decades, the DPRK has underscored the importance of education in mathematics and science for its citizens. The emphasis on the advancement of science and technology, which has historically been a priority for the Kim regime, is reflected in the investment of resources and personnel into related fields of research. Today's cyber and IT education in the DPRK was founded on this drive for advancement and resulted in an integrated curriculum coordinated with the Workers' Party, research centers, and the military.

- In recent years under Kim Jong Un, the regime has placed increased focus on education and training in IT-related subjects and has developed strong IT degree programs at several premier DPRK educational institutions—particularly Kim Il Sung University, Kim Chaek University of Technology, and Pyongyang University of Science and Technology. Approximately 30,000 students study information and communications technology-related subjects at these top universities alone.

- As of 2019, 37 universities had reportedly established 85 programs offering courses in advanced science, technology, engineering, and math (STEM) subjects, including information security, and each province had established at least one new secondary school to cultivate promising students.

- The DPRK education system is highly competitive, and only the top students are accepted into the elite science and technology programs. Students are recruited at a young age from secondary schools like Kumsong Academy and Kumsong Middle School Number 1.

- DPRK IT workers receive additional training overseas and from their own organizations, often through regional IT research centers within the DPRK to further develop their skills. DPRK IT workers have historically received training in East Africa, Southeast Asia, and South Asia and benefit considerably from their overseas training.

HOW DPRK IT WORKERS OPERATE

DPRK IT workers target freelance contracts from employers located in wealthier nations, including those in North America, Europe, and East Asia. In many cases, DPRK IT workers present themselves as South Korean, Chinese, Japanese, or Eastern European, and U.S.-based teleworkers.

In some cases, DPRK IT workers further obfuscate their identities by creating arrangements with third-party sub-contractors. These sub-contractors are non-North Korean, freelance IT workers who complete contracts for the DPRK IT workers. DPRK IT managers have also hired their own teams of non-North Korean IT workers who are usually unaware of the real identity of their North Korean employer or the fact that their employer is a DPRK company. The DPRK IT managers use their outsourced employees to make software purchases and interact with customers in situations that might otherwise expose a DPRK IT worker.

Although DPRK IT workers normally engage in non-malicious IT work, such as the development of a virtual currency exchange or a website, they have used the privileged access gained as contractors to enable DPRK's malicious cyber intrusions. Some overseas-based DPRK IT workers have provided logistical support to DPRK-based malicious cyber actors, although the IT workers are unlikely to be involved in malicious cyber activities themselves. DPRK IT workers may share access to virtual infrastructure, facilitate sales of data stolen by DPRK cyber actors, or assist with the DPRK's money-laundering and virtual currency transfers.

DPRK IT workers have also assisted DPRK officials in procuring WMD and ballistic missile-related items for the DPRK's prohibited weapons programs.

There are instances where workers are subjected to human trafficking, including forced labor. Credible reports show many DPRK workers overseas are subjected to excessive work hours, constant and close surveillance by North Korean government security agents, unsafe and unsanitary living

conditions, and little freedom of movement. The North Korean government withholds up to 90 percent of wages of overseas workers which generates an annual revenue to the government of hundreds of millions of dollars.

DPRK IT Workers: Skills and Platforms

DPRK IT teams abroad most commonly obtain freelance jobs through various online platforms. Companies use these platforms to advertise contracts for projects that freelance IT developers can bid on. Less commonly, the DPRK IT teams find local, non-DPRK nationals to serve as the nominal heads of companies that are actually controlled by North Koreans. There have also been instances in which DPRK IT teams appear, on paper, to work for a legitimate local company but pursue their own business independently – and in return for hiding their North Korean origins, the DPRK IT team will pay a fee to the foreign company. DPRK IT teams often include members proficient in a foreign language, such as English or Chinese.

DPRK IT workers use a wide variety of mainstream and IT industry-specific freelance contracting platforms, software development tools and platforms, messaging applications, and social media and networking websites to obtain development contracts for companies around the world, as well as utilizing a number of digital payment platforms and websites to receive payment for their work. 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 and move funds they receive.

DPRK IT Workers: Hiding Their Identity

DPRK IT workers deliberately obfuscate their identities, locations, and nationality online, often using non-Korean names as aliases. They will also use virtual private networks (VPNs), virtual private servers (VPSs), or utilized third-country IP addresses to appear as though they are connecting to the internet from inconspicuous locations and reduce the likelihood of scrutiny of their DPRK location or relationships. DPRK IT workers generally rely on the anonymity of telework arrangements, use proxies for account creation and maintenance, and favor the use of intermediaries and communications through text-based chat instead of video calls.

DPRK IT workers use proxy accounts to bid on, win, work on, and get paid for projects on freelance software developer websites. These proxy accounts belong to third-party individuals, some of whom sell their identification and account information to the DPRK IT workers. In some cases, DPRK IT workers pay fees to these individuals for use of their legitimate platform accounts. DPRK IT workers may populate freelance platform profiles with the real affiliations and work experience of the proxy.

At times, DPRK IT workers engage other non-North Korean freelance workers on platforms to propose collaboration on development projects. A DPRK IT worker takes advantage of these business relationships to gain access to new contracts and virtual currency accounts used to conduct the IT work over U.S. or European virtual infrastructure, bypassing security measures intended to prevent

fraudulent use. In establishing accounts with the aid of other freelance workers, DPRK IT workers may claim to be third-country nationals who need U.S. or other Western identification documents and freelance platform accounts to earn more money.

Hiding their real locations allows DPRK IT workers to violate terms of service agreements for the online platforms and services they use for their activities. As part of their tradecraft, DPRK IT workers may also use single, dedicated devices for each of their accounts, especially for banking services, to evade detection by fraud prevention, sanctions compliance, and anti-money laundering measures.

DPRK IT workers routinely use counterfeit, altered, or falsified documents, including identification documents, and forged signatures—either that they have made themselves using software such as Photoshop, or that they have paid a document forgery company to alter, combining the IT worker's own or a provided photo with the identifying information of a real person. DPRK IT workers commonly procure forged documents such as:

- driver's licenses,
- social security cards,
- passports,
- national identification cards,
- resident foreigner cards,
- high school and university diplomas,
- work visas, and
- credit card, bank, and utility statements.

In some instances, these identities are stolen, while in others the DPRK IT workers have solicited a non-North Korean national to set up an account using their own personal information or information to which they have access, after which control of the account is transferred to the DPRK IT workers for a fee. This allows the DPRK IT worker to conceal their identity when bidding on and completing freelance projects for clients online, using the infrastructure of the real account holder via remote desktop access. Each IT worker often uses multiple identities and accounts, which can also be shared between IT workers on the same team. These accounts and identities purport to be from countries from every part of the world.

DPRK IT workers may steal the customer account information of U.S. or international banks to verify their identities with freelance platforms, payment providers, and companies employing the DPRK IT workers. In at least one case, DPRK IT workers forged checks using stolen bank account information. Accounts and resumes associated with DPRK IT worker's proxy identities often include falsified, but realistic and detailed education and employment history information, including false contact information for educational institutions and previous employers.

DPRK IT workers may also populate their online developer profiles' employment sections with the names of small or mid-sized Western companies so that the DPRK IT workers appear to be reputable Americans or Europeans when bidding on projects. They may use the names of actual employees and email addresses that appear similar to the Western company's legitimate domain.

DPRK IT workers additionally falsify statement of work agreements, invoices, client communication documentation, and other documents for use with freelancing platforms, likely to satisfy know-your-customer and anti-money laundering (KYC/AML) measures or similar procedures that platforms have in place to ensure the legitimacy of user activity. These falsified documents may have minimal contact details to deter verification.

DPRK IT workers may also attempt to mask their nationality by representing themselves as South Korean or simply "Korean" citizens.

DPRK IT workers who obtain freelance positions with an unwitting company have also been known to subsequently recommend to the company the freelance employment of additional DPRK IT workers.

Resume of a DPRK IT Worker

DPRK IT workers advertise skills working on system and program development, database management systems, and use of a wide variety of common languages, frameworks, tools, and cloud resources. These often include strong skills in a number of coding and markup languages. A majority of DPRK IT worker projects are related to mobile and web app development. DPRK IT workers also use collaborative platforms and hosting services for data and workflow management. These workers often report experience with a variety of databases and are familiar with the cloud and analytics products and services from major providers. Additionally, DPRK IT workers incorporate digital payment and e-commerce platforms in their work.

DPRK IT workers build "portfolio" websites, generally simple in design, in an effort to boost the credibility of their fabricated, freelance developer personas. These virtual portfolios represent the work of DPRK IT workers' personas and are often linked to their online freelance developer accounts. Information on these websites, including contact information and location, as well as work history and education, is likely to be false.

RED FLAG INDICATORS

Freelance work and payment platform companies should be aware of the following activity that may be indications or behaviors of DPRK IT workers who may be using their platforms.

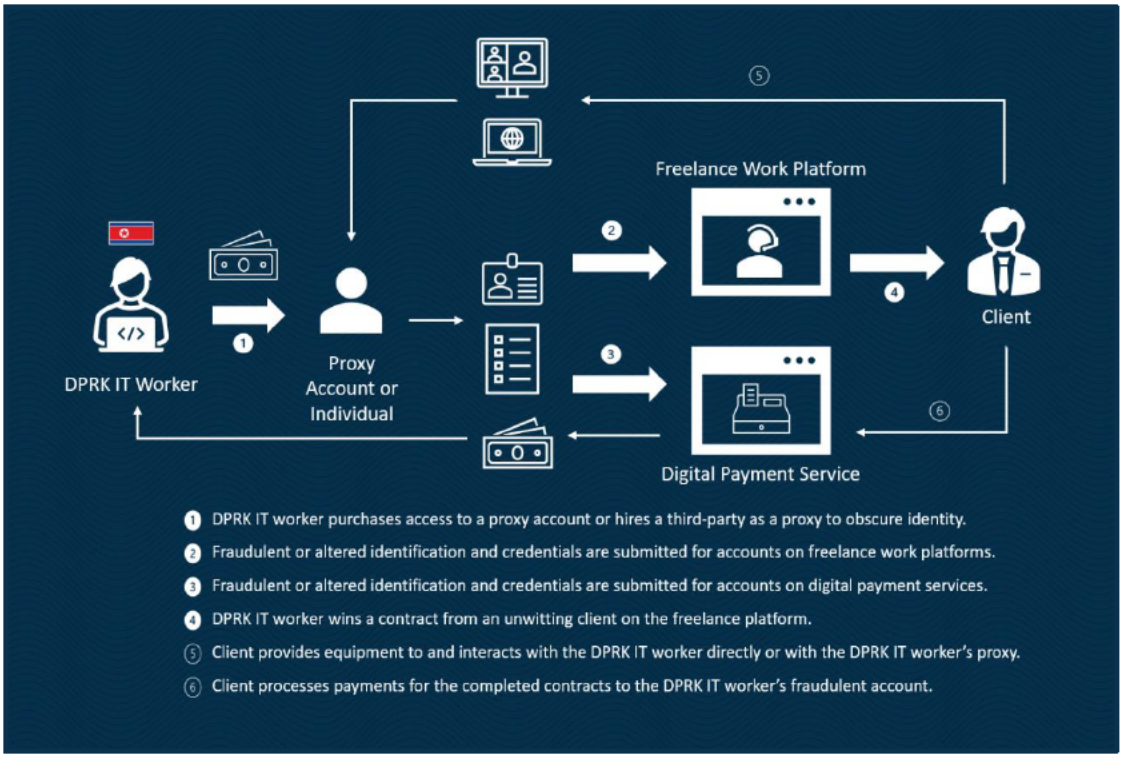
- Multiple logins into one account from various IP addresses in a relatively short period of time, especially if the IP addresses are associated with different countries;
- Developers are logging into multiple accounts on the same platform from one IP address;
- Developers are logged into their accounts continuously for one or more days at a time;
- Router port or other technical configurations associated with use of remote desktop sharing software, such as port 3389 in the router used to access the account, particularly if usage of remote desktop sharing software is not standard company practice;
- Developer accounts use a fraudulent client account to increase developer account ratings, but both the client and developer accounts use the same PayPal account to transfer/withdraw money (paying themselves with their own money);
- Frequent use of document templates for things such as bidding documents and project communication methods, especially the same templates being used across different developer accounts;
- Multiple developer accounts receiving high ratings from one client account in a short period, with similar or identical documentation used to establish the developer accounts and/or the client account;
- Extensive bidding on projects, and a low number of accepted project bids compared to the number of projects bids on by a developer; and
- Frequent transfers of money through payment platforms, especially to PRC-based bank accounts, and sometimes routed through one or more companies to disguise the ultimate destination of the funds.

Companies employing freelance developers should be aware of the following activity that may be indications or behaviors of DPRK IT workers.

- If a freelance software development website or payment platform account has been shut down or the worker contacts the employer requesting use of a different account, especially if registered to a different name;
- Use of digital payment services, especially PRC-linked services;

- 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;
- Surprisingly simple portfolio websites, social media profiles, or developer profiles;
- Direct messaging or cold-calls from individuals purporting to be C-suite level executives of software development companies to solicit services or advertise proficiencies;
- Requests to communicate with clients and potential clients on a separate platform than the original freelance platform website where the client found the IT worker;
- An employer proposes to send documents or work-related equipment such as a laptop to a developer, and the developer requests that items be sent to an address not listed on the developer's identification documentation. Be particularly suspicious if a developer claims they cannot receive items at the address on their identification documentation;
- Seeking payment in virtual currency in an effort to evade KYC/AML measures and use of the formal financial system;
- Requesting payment for contracts without meeting production benchmarks or check-in meetings;
- Inability to conduct business during required business hours;
- Incorrect or changing contact information, specifically phone numbers and emails;
- Biographical information which does not appear to match the applicant;
- Failure to complete tasks in a timely manner or to respond to tasks;
- Inability to reach them in a timely manner, especially through "instant" communication methods; and
- Asking co-workers to borrow some of their personal information to obtain other contracts.

Overview of DPRK IT Worker Operations



POTENTIAL MITIGATION MEASURES

For freelance work and payment platform companies

- Verify documents submitted as part of proposal reviews and contracting due-diligence procedures, such as independently verifying invoices and work agreements by contacting the listed clients using contact information given in business databases and not the contact information provided on the submitted documentation;
- Closely scrutinize identity verification documents submitted for forgery, potentially reaching out to local law enforcement for assistance. Reject low-quality images submitted to provide verification of identity;
- Verify the existence of any websites provided to establish accounts; enhance scrutiny for any accounts that have utilized defunct websites to establish the accounts.
- As part of initial due diligence contracting processes and refresh policies, require submission of a video verifying identity or conduct a video interview to verify identity;

- Regularly use port checking capabilities to determine if the platform is being accessed remotely via desktop sharing software or a VPN or VPS, particularly if usage of remote desktop sharing software or VPN services to access accounts is not standard practice;

- Automatically flag for additional review client and developer accounts that use the same or similar documentation to establish the accounts or that use the same digital payment service accounts;

- Automatically flag for additional review the use of the same or similar document templates for bidding and project communication across different developer accounts;

- Automatically flag for additional review multiple developer accounts receiving high ratings from a single client account in a short period, especially if similar or identical documentation was used to establish the accounts;

- Automatically flag for additional review developer accounts with high bidding rates as well as accounts with a low number of accepted project bids compared to the number of project bids. Additionally, flag accounts with a high number of project bids relative to number of account logins;

- Do not allow any activity in newly established accounts prior to full account verification;

- Provide extra scrutiny to newly established accounts; and

For companies hiring programmers and developers on freelance platforms

- Conduct video interviews to verify a potential freelance worker's identity;

- Conduct a pre-employment background check, drug test, and fingerprint/biometric log-in to verify identity and claimed location. Avoid payments in virtual currency and require verification of banking information corresponding to other identifying documents;

- Use extra caution when interacting with freelance developers through remote collaboration applications, such as remote desktop applications. Consider disabling remote collaboration applications on any computer supplied to a freelance developer;

- Verify employment and higher education history directly with the listed companies and educational institutions, using contact information identified through a search engine or other business database, not directly obtained from the potential employee or from their profile;

- 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. Be extra cautious of simple portfolio websites, social media profiles, or developer profiles;

- Be cautious of a developer requesting to communicate on a separate platform outside the original freelance platform website where a company initially found the IT worker;
- If sending to a developer documents or work-related equipment such as a laptop, only send to the address listed on the developer's identification documents and obtain additional documentation if the developer requests that the laptop or other items be sent to an unfamiliar address. Be suspicious if a developer cannot receive items at the address on their identification documentation; and
- Be vigilant for unauthorized, small-scale transactions that may be fraudulently conducted by contracted IT workers. In one case, DPRK IT workers employed as developers by a U.S. company fraudulently charged the U.S. company's payment account and stole over USD 50,000 in 30 small installments over a matter of months. The U.S. company was not aware the developers were North Korean or of the ongoing theft activity due to the slight amounts.

CONSEQUENCES OF ENGAGING IN PROHIBITED OR SANCTIONABLE CONDUCT

Individuals and entities engaged in or supporting DPRK IT worker-related activity, including processing related financial transactions, should be aware of the potential legal consequences of engaging in prohibited or sanctionable conduct.

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. UN Security Council resolution 2375 prohibits UN Member States from providing new work authorizations, or renewing expired authorizations, for DPRK nationals in their jurisdictions in connection with admission to their territories unless approved in advance by the UN Security Council's 1718 Committee. UN Security Council resolution 2397 requires all Member States to repatriate, by December 22, 2019, DPRK nationals earning income in their jurisdiction—regardless of when or whether work authorizations were issued for the DPRK nationals in question.

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 of Korea that undermine cybersecurity;
- Operated on behalf of the DPRK in the IT industry;
- Engaged in certain other malicious cyber-enabled activities;

- Engaged in at least one significant importation from or exportation to the DPRK of any goods, services, or technology;

- Sold, supplied, transferred, or purchased, directly or indirectly, to or from the DPRK or any person acting for or on behalf of the Government of the DPRK or the Workers' Party of Korea, software, where any revenue or goods received may benefit the Government of the DPRK or the Workers' Party of Korea; or

- Materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the Government of the DPRK or the Workers' Party of Korea.

For example, in 2018, the United States designated for sanctions the China-based technology firm Yanbian Silverstar Network Technology Co., Ltd. This company was nominally a Chinese IT company, but in reality it was managed and controlled by North Koreans. This company also created a Russia-based front company, Volasys Silver Star, to circumvent identification requirements on freelance job forums.

Additionally, if the Secretary of the Treasury, in consultation with the Secretary of State, determines that a foreign financial institution has knowingly conducted or facilitated significant trade with the DPRK, or knowingly conducted or facilitated a significant transaction on behalf of a person designated under a DPRK-related Executive Order, or under Executive Order 13382 (Weapons of Mass Destruction Proliferators and Their Supporters) for DPRK-related activity, that institution may, among other potential restrictions, lose the ability to maintain a correspondent or payable-through account in the United States.

OFAC investigates apparent violations of its sanctions regulations and exercises enforcement authority, as outlined in the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, appendix A. Persons who violate the North Korea Sanctions Regulations, 31 C.F.R. part 510, may face civil monetary penalties of up to the greater of the applicable statutory maximum penalty or twice the value of the underlying transaction.

In addition, the Countering America's Adversaries Through Sanctions Act (CAATSA; Public Law 115-44) Section 321(b) (22 U.S.C. § 9241a), which amended the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. § 9241 et seq.), created a rebuttable presumption that significant goods, wares, merchandise, and articles mined, produced, or manufactured wholly or in part by North Korean nationals or North Korean citizens anywhere in the world are forced-labor goods prohibited from importation under the Tariff Act of 1930 (19 U.S.C. § 1307). This means that these goods shall not be entitled to entry at any port of the United States and may be subject to detention, seizure, and forfeiture. Violations may result in civil penalties, as well as criminal prosecution. However, pursuant to CAATSA, such goods may be imported into the United States if the Commissioner of U.S. Customs and Border Protection (CBP) finds by clear and convincing evidence that the goods were not

produced with convict labor, forced labor, or indentured labor. The prohibition against the importation of goods produced with convict labor, forced labor, or indentured labor under penal sanctions (including forced or indentured child labor) was created under the Tariff Act of 1930, and as such, has been in place for nearly 90 years.

The Department of Justice is responsible for the investigation and prosecution of applicable federal laws, including the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701 et seq., and the Bank Secrecy Act (BSA), 31 U.S.C. §§ 5318 and 5322. Under IEEPA, it is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issues pursuant to IEEPA, to include any DPRK-related Executive Order (e.g., Executive Orders 13722 and 13810), Executive Order 13382, and the North Korean Sanctions Regulations, 31 C.F.R. part 510. Persons who willfully violate IEEPA face up to 20 years' imprisonment, fines of up to $1 million or totaling twice the gross gain, whichever is greater, and potential forfeiture of all funds involved in such transactions. The BSA requires financial institutions to, among other things, maintain effective anti-money laundering programs and file certain reports with FinCEN. Persons violating the BSA may face up to 5 years' imprisonment, a fine of up to $250,000, and potential forfeiture of property involved in such violations. Corporations and other entities that violate IEEPA, the BSA, and other applicable federal laws may also be criminally prosecuted. The Department of Justice also works with foreign partners to share evidence in support of criminal investigations and prosecutions in the United States and abroad.

Pursuant to 31 U.S.C. § 5318(k), the Secretary of the Treasury or the Attorney General may subpoena a foreign financial institution that maintains a correspondent bank account in the United States for records stored overseas. Where the Secretary of the Treasury or Attorney General provides written notice to a U.S. financial institution that a foreign financial institution has failed to comply with such a subpoena, the U.S. financial institution must terminate the correspondent banking relationship within ten business days. Failure to do so may subject the U.S. financial institutions to daily civil penalties.

DPRK REWARDS FOR JUSTICE

If you have information about illicit DPRK activities in cyberspace, including past or ongoing operations, providing such information through the Department of State's Rewards for Justice program could make you eligible to receive an award of up to $5 million. For further details, please visit https://rewardsforjustice.net/index/?north-korea=north-korea.

ANNEX

United Nations Panel of Experts Reporting on DPRK IT Workers

The UN Security Council 1718 Sanctions Committee on the DPRK is supported by a Panel of Experts (the Panel) who gather, examine, and analyze information from UN Member States, relevant UN bodies, and other parties on the implementation of the measures outlined in the UN Security Council Resolutions addressing the DPRK. The Panel also makes recommendations on how to improve sanctions implementation by providing both a midterm and a final report to the 1718 Committee. These reports can be found at:
https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports

The Panel has investigated multiple cases of DPRK IT workers, such as those subordinate to the UN-designated Munitions Industry Department (MID), and presented information on these investigations in the Panel's semi-annual reports, including the following:

The Panel first reported on DPRK IT workers in its 2019 Midterm Report, noting that the MID, which had been designated for its supervisory role in the development of the DPRK's nuclear and ballistic missile programs, 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. At the time, DPRK IT workers located in Europe, Asia, Africa, and the Middle East utilized foreign websites to obtain freelance work while disguising their identities. Alongside non-malicious information technology work, DPRK IT workers conducted illicit work involving the theft of assets such as virtual currencies in support of DPRK cyber actors in the evasion of financial sanctions.

The Panel continued its investigation into DPRK IT workers in its 2020 Final Report, finding that most overseas DPRK IT workers are employed by companies subordinate to MID. By 2019, the MID was suspected of having dispatched at least 1,000 IT workers overseas for the purpose of revenue generation, often using subordinate entities or front companies. However, due to their obfuscation techniques, the true number of IT workers abroad and in the DPRK was unclear. The Panel noted that DPRK IT workers use several methods to obtain freelance IT work without revealing their identity, including by setting up accounts on freelance developer platforms with unwitting clients around the world, especially in China, Russia, Ukraine, Serbia, Canada, and the United States. The Panel further investigated several specific cases of DPRK IT worker teams and associated companies in China, Nepal, and Vietnam.

The Panel investigated a number of DPRK IT worker teams in China and Russia, detailing their investigations in its 2020 Midterm Report. The Panel noted that hundreds of DPRK IT workers subordinate to MID were operating in China in 2019 and 2020, illicitly gaining access to freelance platform accounts in the names of third-country individuals. The Panel further noted that multiple groups of DPRK MID-subordinate IT workers were operating in Russia in 2019 and 2020, utilizing

false, foreign identities to access information technology freelance platforms, virtual currency websites, and payment websites.

According to the Panel's 2021 Final Report, 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. The Panel further noted that most accounts linked to the DPRK operate from locations in China. To avoid scrutiny, these accounts will go "off-site" after establishing contact with potential customers seeking to hire IT services. DPRK-linked users also target IT freelance platforms with lower levels of security or less rigorous due diligence procedures. The Panel specifically highlighted the dangers facing IT freelance platforms in performing compliance obligations and unintentionally facilitating DPRK access to international payment systems, recommending that UN Member States work with freelance IT companies to promote and enhance sanctions compliance implementation capacity and capability.