WASHINGTON — Today, the Department of the Treasury’s Office of Foreign Assets Control (OFAC) sanctioned four entities and one individual involved in obfuscated revenue generation and malicious cyber activities that support the Democratic People’s Republic of Korea (DPRK) Government. The DPRK conducts malicious cyber activities and deploys information technology (IT) workers who fraudulently obtain employment to generate revenue, including in virtual currency, to support the Kim regime and its priorities, such as its unlawful weapons of mass destruction and ballistic missile programs.

“Today’s action continues to highlight the DPRK’s extensive illicit cyber and IT worker operations, which finance the regime’s unlawful weapons of mass destruction and ballistic missile programs,” said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. “The United States and our partners remain committed to combatting the DPRK’s illicit revenue generation activities and continued efforts to steal money from financial institutions, virtual currency exchanges, companies, and private individuals around the world.”

Today’s actions demonstrate our continued coordination with our Republic of Korea (ROK) partners, who are concurrently taking sanctions action against overseas DPRK IT workers, by jointly designating the individual and one of the entities identified below. Furthermore, the other three entities OFAC is designating today were previously sanctioned by the ROK on February 10, 2023, for engaging in cyber operations and illicit revenue generation that support the DPRK’s WMD programs.

**DPRK MALICIOUS CYBER ORGANIZATIONS**

The DPRK’s malicious cyber actors target individuals and companies worldwide to steal funds to support the regime’s priorities, including its unlawful weapons of mass destruction (WMD) and ballistic missile programs. According to a March 2023 UN Panel of Experts report, DPRK cyber actors stole more virtual currency in 2022 than in any previous year, with estimates ranging from $630 million to over $1 billion—reportedly doubling Pyongyang’s total cyber theft proceeds in 2021.
Pyongyang University of Automation, one of the DPRK’s premier cyber instruction institutions, is responsible for training malicious cyber actors, many of whom go on to work in cyber units subordinate to the Reconnaissance General Bureau (RGB)—the DPRK’s primary intelligence bureau and main entity responsible for the country’s malicious cyber activities. The RGB was designated by OFAC on January 2, 2015, for being a controlled entity of the Government of North Korea pursuant to Executive Order (E.O.) 13687.

OFAC is also designating the RGB-controlled Technical Reconnaissance Bureau and its subordinate cyber unit, the 110th Research Center. The DPRK-based Technical Reconnaissance Bureau leads the DPRK’s development of offensive cyber tactics and tools and operates several departments, including those affiliated with the Lazarus Group. On March 23, 2022, the Lazarus Group carried out the largest virtual currency heist to date, stealing about $620 million in virtual currency from a blockchain project linked to the online game Axie Infinity. The Lazarus Group was designated by OFAC on September 13, 2019, as an agency, instrumentality, or controlled entity of the Government of North Korea pursuant to E.O. 13722.

The 110th Research Center has conducted cyber operations against networks worldwide, including in the United States and the ROK. In 2013, the 110th Research Center conducted the campaign known as DarkSeoul, which destroyed thousands of financial sector systems and resulted in outages at the top three media companies in the ROK. Additionally, the 110th Research Center has stolen sensitive government information from the ROK related to its military defense and response planning.

Pyongyang University of Automation, Technical Reconnaissance Bureau, and the 110th Research Center are being designated pursuant to E.O. 13687 for being agencies, instrumentalities, or controlled entities of the Government of North Korea or the Workers’ Party of Korea.

ILLEGAL IT WORKER REVENUE GENERATION

In addition to theft resulting from cyber intrusions, the DPRK generates significant revenue through the deployment of IT workers who fraudulently obtain employment with companies around the world, including in the technology and virtual currency industries. The DPRK maintains a workforce of thousands of highly skilled IT workers around the world, primarily located in the People’s Republic of China and Russia, to generate revenue that contributes to its unlawful WMD and ballistic missile programs. In some cases, DPRK IT workers can each earn more than $300,000 per year. These 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 at these companies. They target employers located in wealthier
countries, utilizing a variety of mainstream and industry-specific freelance contracting, payment, and social media and networking platforms. 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. 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.

The vast majority of DPRK IT workers are subordinate to, and working on behalf of, UN- and U.S.-designated DPRK entities directly involved in Pyongyang’s unlawful WMD and ballistic missile programs; this IT worker activity has included assisting DPRK officials in procuring WMD and ballistic missile-related items. Although these workers normally engage in IT work distinct from malicious cyber activity, we have also seen instances in which DPRK IT workers have provided some support to the DPRK's malicious cyber program through privileged access to virtual currency firms.

DPRK-based **Chinyong Information Technology Cooperation Company** (Chinyong), also known as Jinyong IT Cooperation Company, is associated with the UN- and U.S.-sanctioned Ministry of Peoples’ Armed Forces. Chinyong, by way of companies under its control and their representatives, employs delegations of DPRK IT workers that operate in Russia and Laos. One such representative of the Chinyong office located in Vladivostok, Russia, DPRK-national **Kim Sang Man (Kim)**, is presumed to be involved in the payment of salaries to family members of Chinyong’s overseas DPRK worker delegations.

Furthermore, Kim has been involved in the sale and transfer of IT equipment for the DPRK and, as recently as 2021, received cryptocurrency funds transfers from IT teams located in China and Russia that were valued at more than $2 million USD. Kim maintained awareness of cryptocurrency payments from a company under his leadership that were being sent to the DPRK. Kim has been affiliated with the U.S.-designated Korea Computer Center and worked as an IT developer in the DPRK prior to being selected as an agent of the UN- and U.S.-designated RGB, in order to earn foreign currency.

Chinyong is being designated pursuant to E.O. 13687 for being an agency, instrumentality, or controlled entity of the Government of North Korea or the Workers’ Party of Korea.

Kim is being designated pursuant to E.O. 13810 for being a North Korean person, including a North Korean person that has engaged in commercial activity that generates revenue for the Government of North Korea or the Workers’ Party of Korea.
Today, the ROK is also designating Chinyong and Kim in relation to their IT worker activities.

**SANCTIONS IMPLICATIONS**

As a result of today’s action, pursuant to E.O. 13687 and E.O. 13810, all property and interests in property of the persons named above that are in the United States, or in the possession or control of U.S. persons, are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked.

In addition, persons that engage in certain transactions with the individuals or entities designated today may themselves be exposed to designation. Furthermore, any foreign financial institution that knowingly facilitates a significant transaction or provides significant financial services for any of the individuals or entities designated today could be subject to U.S. correspondent or payable-through account sanctions.

The power and integrity of OFAC sanctions derive not only from OFAC’s ability to designate and add persons to the Specially Designated Nationals and Blocked Persons (SDN) List but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to OFAC’s Frequently Asked Question 897.

For additional information regarding the DPRK’s IT workers, see the May 16, 2022, Guidance on the Democratic People’s Republic of Korea Information Technology Workers.

For guidance on complying with sanctions as they relate to virtual currency, see OFAC’s Sanctions Compliance Guidance for the Virtual Currency Industry and OFAC’s FAQs on virtual currency.

For detailed information on the process to submit a request for removal from an OFAC sanctions list.

Find identifying information on the individuals and entities sanctioned today here.

###