Sanctions Imposed on DPRK IT Workers Generating Revenue for the Kim Regime

Published: 2026-02-13 · Archived: 2026-04-05 22:53:10 UTC

WASHINGTON — Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned **Song Kum Hyok**, (**Song**), a malicious cyber actor associated with the sanctioned Democratic People's Republic of Korea (DPRK) Reconnaissance General Bureau (RGB) hacking group Andariel.

Song facilitated an information technology (IT) worker scheme in which individuals, often DPRK nationals working from countries such as China and Russia, were recruited and provided with falsified identities and nationalities to obtain employment at unwitting companies to generate revenue for the DPRK regime. In some cases, these DPRK IT workers have been known to introduce malware into company networks for additional exploitation. OFAC is also sanctioning one individual and four entities involved in a Russia-based IT worker scheme that has generated revenue for the DPRK.

"Today's action underscores the importance of vigilance on the DPRK's continued efforts to clandestinely fund its WMD and ballistic missile programs," said **Deputy Secretary of the Treasury Michael Faulkender**. "Treasury remains committed to using all available tools to disrupt the Kim regime's efforts to circumvent sanctions through its digital asset theft, attempted impersonation of Americans, and malicious cyber-attacks."

Today's designation is part of the U.S. government's objective to counter the DPRK's efforts to advance its strategic goals through cyber espionage and revenue generation. On March 2, 2016, the United Nations Security Council (UNSC) adopted Resolution 2270 designating the RGB for its role supporting the Kim regime's unlawful weapons development. Today's action reaffirms that relevant UNSC resolutions remain in full force. On September 13, 2019, OFAC designated the Lazarus Group, Bluenoroff, and Andariel: all DPRK-sponsored cyber groups subordinate to the RGB, which have carried out numerous high-value virtual currency heists to offset the impact of U.S. and multilateral sanctions. Additionally, on May 23, 2023, OFAC designated the Technical Reconnaissance Bureau, which leads the DPRK's development of offensive cyber tactics and tools, and its subordinate cyber unit, the 110th Research Center.

Illicit DPRK IT Worker SchemeS

The DPRK generates significant revenue through the deployment of IT workers who fraudulently gain 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 globally, primarily located in the People's Republic of China and Russia, who generate significant revenue that contributes to its WMD and ballistic missile programs.

These workers are instructed to deliberately obfuscate their identities, locations, and nationalities, typically using false 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, and they use virtual currency exchanges and trading platforms to manage funds they receive for contract work as well as to launder and remit these funds to the DPRK.

KEY FACILIATOR FOR KIM REGIME'S OVERSEAS IT WORKFORCE

Song is a DPRK-based cyber actor who used foreign-hired IT workers to seek remote employment with U.S. companies and planned to split income with them. In 2022 and 2023, **Song** used U.S. persons' information, including names, social security numbers, and addresses to create aliases for the hired foreign workers. The workers then used the accounts to pose as U.S. persons looking for remote jobs with U.S. companies.

Song is being designated pursuant to Executive Order (E.O.) 13694, as further amended by E.O. 14306, for being responsible for or complicit in, or having engaged in, directly or indirectly, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of funds or economic resources, intellectual property, proprietary or business confidential information, personal identifiers, or financial information misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such funds or economic resources, intellectual property, proprietary or business confidential information, personal identifiers, or financial information is reasonably likely to result in, or has materially contributed to, a threat to the national security, foreign policy, or economic health or financial stability of the United States.

ASATRYAN IT WORKER NETWORK

Gayk Asatryan (Asatryan), a Russian national, has used his Russia-based companies to employ North Korean IT workers. In mid-2024, Asatryan signed a 10-year contract with a DPRK company, **Korea Songkwang Trading General Corporation** (Songkwang Trading), to dispatch up to 30 DPRK IT workers to work in Russia for his company, **Asatryan Limited Liability Company** (Asatryan LLC). Asatryan also signed a contract with DPRK company **Korea Saenal Trading Corporation** (Saenal Trading), in which they planned to dispatch 50 DPRK IT workers to Russia for his company, **Fortuna Limited Liability Company** (Fortuna LLC).

OFAC designated Asatryan pursuant to E.O. 13722 for having attempted to engage in, facilitate, or be responsible for the exportation of workers from North Korea, including exportation to generate revenue for the Government of North Korea or Workers' Party of Korea. Asatryan LLC and Fortuna LLC are designated pursuant to E.O. 13722 for being owned or controlled by or acting or purporting to act for or on behalf of, directly or indirectly, Asatryan, a person whose property and interests in property are blocked pursuant to E.O. 13722. Songkwang Trading and Saenal Trading are designated pursuant to E.O. 13810 for being North Korean persons, including North Korean persons that have engaged in commercial activity that generates revenue for the Government of North Korea or Workers' Party of Korea.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated or blocked persons described 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, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by a general or specific license issued by OFAC, or exempt, OFAC's regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of blocked persons.

Violations of U.S. sanctions may result in the imposition of civil or criminal penalties on U.S. and foreign persons. OFAC may impose civil penalties for sanctions violations on a strict liability basis. OFAC's Economic Sanctions Enforcement Guidelines provide more information regarding OFAC's enforcement of U.S. economic sanctions. In addition, financial institutions and other persons may risk exposure to sanctions for engaging in certain transactions or activities involving designated or otherwise blocked persons. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any designated or blocked person, or the receipt of any contribution or provision of funds, goods, or services from any such person.

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 List (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, or to submit a request, please refer to OFAC's guidance on Filing a Petition for Removal from an OFAC List.

For more information on the individuals and entity designated today, click here.

To read the DPRK IT Workers Advisory, click here.
