OpenVoiceNews U.S.

Transparent. Unbiased. Yours.

US Sanctions Russian, DPRK Fake IT Worker Network

July 10, 2025
— Categories: Defence & Security

The United States has taken strong action to disrupt an elaborate scheme that used fake identities and shadow companies to funnel money back to North Korea’s government. On Tuesday, the United States Department of the Treasury’s Office of Foreign Assets Control (OFAC) announced sanctions targeting two individuals and four companies accused of orchestrating the operation.

According to OFAC, the network relied on North Korean information technology workers who posed as Americans to get remote jobs at US companies. The workers used stolen names, Social Security numbers, and addresses to apply for these positions, often appearing no different than any other freelance contractor. But behind the scenes, their earnings were channeled directly to support the Democratic People's Republic of Korea (DPRK) regime.

One of the sanctioned individuals is Song Kum Hyok, a North Korean described as a "malicious cyber actor" linked to the Reconnaissance General Bureau's hacking group Andariel, which has already been sanctioned in the past. OFAC said Song helped set up false identities for these workers, enabling them to secure employment under the radar between 2022 and 2023.

The crackdown also extended to Russian national Gayk Asatryan, who, US officials say, signed long-term contracts with North Korean state-run companies to hire dozens of IT workers in Russia. Earlier this year, Asatryan reportedly agreed to bring on 80 North Korean workers through his firms, Asatryan Limited Liability Company and Fortuna Limited Liability Company.

Officials emphasized that these sanctions will freeze any assets tied to the named individuals and companies, cutting off payments and preventing further profits from reaching Pyongyang. The Treasury designated both the North Korean companies Korea Songkwang Trading General Corporation and Korea Saenal Trading Corporation as part of the scheme to generate revenue for the North Korean government and the Workers' Party of Korea.

Cybersecurity experts have praised the move, noting that it highlights a vulnerability in remote work hiring. "These sanctions are a major step toward closing a long-standing gap in remote-work security," said Fritz Jean-Louis, principal cybersecurity advisor at Info-Tech Research Group. "It shows how easily fake identities and minimal vetting can enable sanctioned regimes to slip into global workforces."

The US government is urging companies to strengthen their hiring processes and conduct thorough due diligence when onboarding remote workers to avoid inadvertently funding prohibited activities.

Download IPFS