

Treasury Sanctions Fraud Network Funding DPRK Weapons Programs

Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned **Vitaliy Sergeyevich Andreyev**, **Kim Ung Sun**, **Shenyang Geumpungri Network Technology Co., Ltd**, and **Korea Sinjin Trading Corporation** for their roles in a fraudulent information technology (IT) worker scheme orchestrated by the Democratic People's Republic of Korea (DPRK) government.

"The North Korean regime continues to target American businesses through fraud schemes involving its overseas IT workers, who steal data and demand ransom," said **Under Secretary of the Treasury for Terrorism and Financial Intelligence John K. Hurley**. "Under President Trump, Treasury is committed to protecting Americans from these schemes and holding the guilty accountable."

DPRK IT WORKFORCE: REVENUE GENERATOR FOR THE REGIME

The DPRK utilizes IT workers to generate revenue for its illicit weapons of mass destruction and ballistic missile programs, in violation of U.S. and United Nations sanctions. The teams of IT workers typically use fraudulent documents, stolen identities, and false personas to deliberately obfuscate their identities and infiltrate legitimate companies, including in the United States and allied countries. The DPRK government claims the majority of the wages earned by these overseas IT workers in order to generate hundreds of millions of dollars for the regime's weapons of mass destruction and ballistic missile programs. In some cases, these DPRK workers have also clandestinely introduced malware into company networks to exfiltrate proprietary and sensitive data. More information about the tactics utilized by DPRK IT workers and steps that can be taken to protect private networks can be found in the January 23, 2025 Federal Bureau of Investigation Public Service Announcement, North Korean IT Workers Conducting Data Extortion.

OVERSEAS IT WORKER NETWORK

OFAC's action today designates an IT worker network that consists of a DPRK-based trading company, a Chinese front company, and two individuals that have provided financial assistance in order to generate revenue for the DPRK regime.

Vitaliy Sergeyevich Andreyev (Andreyev) is a Russian national facilitating payments to U.S.-designated Chinyong Information Technology Cooperation Company (Chinyong), an entity associated with the DPRK defense ministry that employs delegations of IT workers in Russia and Laos. Since at least December 2024, Andreyev has worked with **Kim Ung Sun**, a Russia-based DPRK economic and trade consular official, to facilitate multiple financial transfers worth a total of nearly \$600,000, by converting cryptocurrency to cash in U.S. dollars.

Shenyang Geumpungri Network Technology Co., Ltd (Shenyang Geumpungri) is a Chinese front company for Chinyong, consisting of a delegation of DPRK IT workers. Since 2021, Shenyang Geumpungri's delegation of DPRK IT workers has earned over \$1 million in profits for Chinyong and **Korea Sinjin Trading Corporation** (Sinjin). Sinjin is a DPRK company subordinate to the U.S.-sanctioned DPRK Ministry of People's Armed Forces General Political Bureau.

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.

Dated 27 August, 2025

