Two North Korean Nationals and Three Facilitators Indicted for Multi-Year Fraudulent Remote Information Technology Worker Scheme that Generated Revenue for the Democratic People's Republic of Korea

Published: 2025-01-23 · Archived: 2026-04-05 14:46:48 UTC

Note: View the indictment here.

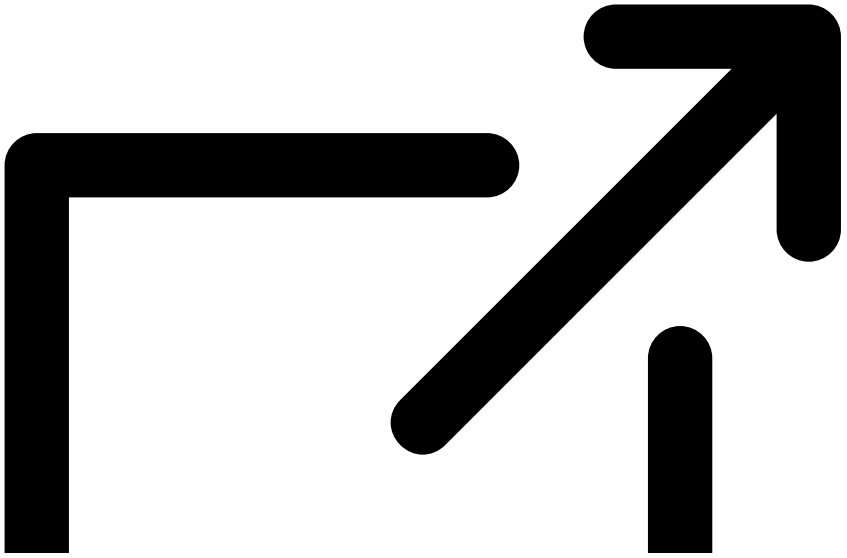
The Justice Department today announced the indictment of North Korean nationals Jin Sung-Il (진성일) and Pak Jin-Song (박진성), Mexican national Pedro Ernesto Alonso De Los Reyes, and U.S. nationals Erick Ntekereze Prince and Emanuel Ashtor for a fraudulent scheme to obtain remote information technology (IT) work with U.S. companies that generated revenue for the Democratic People's Republic of Korea (DPRK or North Korea).

"The Department of Justice remains committed to disrupting North Korea's cyber-enabled sanctions-evading schemes, which seek to trick U.S. companies into funding the North Korean regime's priorities, including its weapons programs," said Supervisory Official Devin DeBacker of the Justice Department's National Security Division. "Our commitment includes the vigorous pursuit of both the North Korean actors and those providing them with material support. It also includes standing side-by-side with U.S. companies to not only disrupt ongoing victimization, but also to help them independently detect and prevent such schemes in the future."

"FBI investigation has uncovered a years-long plot to install North Korean IT workers as remote employees to generate revenue for the DPRK regime and evade sanctions," said Assistant Director Bryan Vorndran of the FBI's Cyber Division. "The indictments announced today should highlight to all American companies the risk posed by the North Korean government. As always, the FBI is available to assist victims of the DPRK. Please reach out to your local FBI field office should you have any questions or concerns."

According to the indictment, over the course of their scheme, from approximately April 2018 through August 2024, the defendants and their unindicted co-conspirators obtained work from at least sixty-four U.S. companies. Payments from ten of those companies generated at least $866,255 in revenue, most of which the defendants then laundered through a Chinese bank account. As part of this prosecution, the FBI arrested Ntekereze and Ashtor and executed a search of Ashtor's residence in North Carolina, where he previously operated a "laptop farm" that hosted victim company-provided laptops to deceive companies into thinking they had hired U.S.-located workers. Alonso was arrested in the Netherlands on Jan. 10, pursuant to an arrest warrant from the United States.

The DPRK has dispatched thousands of skilled IT workers to live abroad, primarily in China and Russia, with the aim of deceiving U.S. and other businesses worldwide into hiring them as freelance IT workers to generate revenue for the regime. DPRK IT worker schemes involve the use of pseudonymous email, social media, payment platform and online job site accounts, as well as false websites, proxy computers, and witting and unwitting third parties located in the United States and elsewhere. As described in a May 2022 tri-seal public service advisory



released by the FBI, and State and Treasury Departments, such IT workers have been known individually earn up to $300,000 annually, generating hundreds of millions of dollars collectively each year, on behalf of designated entities, such as the North Korean Ministry of Defense and others directly involved in the DPRK's weapons of mass destruction programs.

According to the indictment, the defendants used forged and stolen identity documents, including U.S. passports containing the stolen personally identifiable information of a U.S. person, to conceal the true identities of Jin, Pak, and other North Korean co-conspirators, so that these North Korean nationals could circumvent sanctions and other laws to obtain employment with U.S. companies. Ntekereze and Ashtor received laptops from U.S. company employers at their residences, downloading and installing remote access software on them, without authorization, to facilitate IT worker access and to perpetuate the deception of U.S. companies. The defendants further conspired to launder payments for the remote IT work through a variety of accounts designed to promote the scheme and conceal its proceeds.

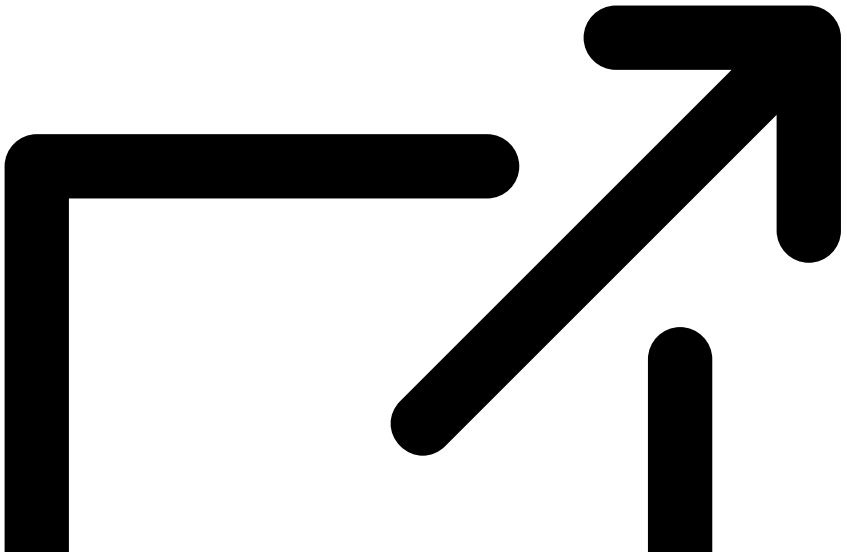
All five defendants are charged with conspiracy to cause damage to a protected computer, conspiracy to commit wire fraud and mail fraud, conspiracy to commit money laundering, and conspiracy to transfer false identification documents. Jin and Pak are charged with conspiracy to violate the International Emergency Economic Powers Act. If convicted, the defendants face a maximum penalty of 20 years in prison. A federal district court judge will determine the sentence of each defendant after considering the U.S. Sentencing Guidelines and other statutory factors.

Under the Department-wide "DPRK RevGen: Domestic Enabler Initiative," launched in March 2024 by the National Security Division and the FBI's Cyber and Counterintelligence Divisions, Department prosecutors and agents are prioritizing the identification and shuttering of U.S.-based "laptop farms" – locations hosting laptops provided by victim U.S. companies to individuals they believed were legitimate U.S.-based freelance IT workers – and the investigation and prosecution of individuals hosting them. Today's announcement follows successful actions taken by the Department in October 2023, May 2024, August 2024, and December 2024, which targeted similar and related conduct.

The FBI Miami Field Office is investigating the case.

Assistant U.S. Attorneys Jonathan Stratton and Sean Cronin for the Southern District of Florida and Trial Attorney Gregory J. Nicosia, Jr. of the National Security Division's National Security Cyber Section are prosecuting the case. Substantial assistance was also provided by Tracy Varghese and Menno Goedman of the National Security Division's Counterintelligence and Export Control Section and the Justice Department's Office of International Affairs.

The FBI, in conjunction with the State and Treasury Departments, issued a May 2022 advisory



to alert the international community, private sector, and public about the North Korea IT worker threat. Updated guidance was issued in October 2023 by the United States and the Republic of Korea (South Korea) and in May 2024 by the FBI, which include indicators to watch for that are consistent with the North Korea IT worker fraud and the use of U.S.-based laptop farms. Today, the FBI issued additional guidance regarding extortion and theft of sensitive company data by North Korean IT workers, along with recommended mitigations.

An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.
