

Treasury Targets North Korea-Controlled Information Technology Companies in China and Russia

September 13, 2018

WASHINGTON – The U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) today announced North Korea-related designations, continuing the implementation of existing sanctions. Today’s action against two entities and one individual targets the revenue North Korea earns from overseas information technology (IT) workers.

“These actions are intended to stop the flow of illicit revenue to North Korea from overseas information technology workers disguising their true identities and hiding behind front companies, aliases, and third-party nationals. Treasury is once again warning the IT industry, businesses, and individuals across the globe to take precautions to ensure that they are not unwittingly employing North Korean workers for technology projects by doing business with companies like the ones designated today,” said Treasury Secretary Steven Mnuchin. “The United States will continue to fully enforce and implement sanctions until we have achieved the final, fully verified denuclearization of North Korea.”

OFAC designated Jilin, China-based **Yanbian Silverstar Network Technology Co., Ltd.** (a.k.a. “**China Silver Star**” or 延边银星网络科技有限公司), its North Korean CEO, **Jong Song Hwa** (정성화), and its Vladivostok, Russia-based sister company, **Volasys Silver Star**.

China Silver Star is nominally a Chinese IT company, but in reality it is managed and controlled by North Koreans. As of mid-2018, **China Silver Star** had earned millions of dollars from collaborative projects with Chinese and other companies. In early 2017, a North Korean IT worker and employee of **China Silver Star** created **Volasys Silver Star** as a Russia-based front company, most likely to facilitate the circumvention of identification requirements on freelance job fora and obfuscate the North Korean workers’ true nationality from clients. In early 2018, **Volasys Silver Star** employees, many of whom had moved to Russia from **China Silver Star**, had earned hundreds of thousands of dollars in under a year. Although nominally run by a Russian individual, **Volasys Silver Star** is also in fact managed by North Koreans. As its CEO, Jong Song Hwa set company goals for **China Silver Star**, and he controls the flow of earnings for several teams of developers in China and Russia.

China Silver Star and **Volasys Silver Star** were each designated under two authorities: for having engaged in, facilitated, or been responsible for the exportation of workers from North Korea, including exportation to generate revenue for the Government of North Korea or the Workers' Party of Korea (E.O. 13722); and for operating in the IT industry in North Korea (E.O. 13810). **Jong Song Hwa** was designated for having acted or purported to act for or on behalf of, directly or indirectly, **China Silver Star**.

The United Nations Security Council acknowledged in Resolution 2397 of 2017 that the revenue generated from North Korean workers overseas contributes to North Korea's nuclear weapons and ballistic missile programs. Indeed, **China Silver Star** is associated with the UN- and U.S.-designated Munitions Industry Department (MID) of the Workers' Part of Korea and the UN- and U.S.-designated Korea Kuryonggang Trading Corporation (Kuryonggang). The MID is responsible for overseeing North Korea's ballistic missile programs, and Kuryonggang is primarily responsible for the procurement of commodities and technologies to support North Korea's defense research and development programs and procurement.

As a result of today's action, any property or interests in property of the designated persons in the possession or control of U.S. persons or within the United States must be blocked, and U.S. persons generally are prohibited from dealing with any of the designated persons.

Furthermore, as noted in the recent [Supply Chain Advisory](#)  issued by the U.S. Department of State, with the U.S. Department of the Treasury and the U.S. Department of Homeland Security, the IT industry, among other industries, has heightened risk of involving North Korean labor. North Korea sells a range of IT services and products abroad, including website and app development, security software, and biometric identification software that have military and law enforcement applications. North Korean firms disguise themselves through a variety of tactics including the use of front companies, aliases, and third-country nationals who act as facilitators. Businesses should be aware of deceptive practices employed by North Korea in order to implement effective due diligence policies, procedures, and internal controls to ensure compliance with applicable legal requirements across their entire supply chains.

[Identifying information on the individual and entities designated today.](#)

####