



ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ



គណៈកម្មការគ្រប់គ្រងល្បែងពាណិជ្ជកម្មកម្ពុជា
អគ្គលេខាធិការដ្ឋាន

បទបញ្ជា

ស្តីពី

**សេចក្តីណែនាំលើបុគ្គលិកបច្ចេកវិទ្យាព័ត៌មាននៃសាធារណរដ្ឋ
ប្រជាធិបតេយ្យប្រជាមានិតកម្ពុជា - ហានិភ័យទប់ក្រហម និងអនុសាសន៍**

រៀបចំដោយ៖ ក្រុមការងារប្រឆាំងការសម្អាតប្រាក់ និងហិរញ្ញប្បទានកេរ្តិ៍ម្តង
ប្រចាំអគ្គលេខាធិការដ្ឋាននៃ គ.ល.ក.

២០២៤

មាតិកា



១. សាវតារនៃសេចក្តីណែនាំ

២. គោលបំណងនៃសេចក្តីណែនាំ

៣. ប្រតិបត្តិការរបស់បុគ្គលិក IT នៃកូរ៉េខាងលើ

៤. សូចនាករទង់ក្រហម Red Flag Indicators

៥. ផលប៉ះពាល់ក្នុងការចូលរួមពាក់ព័ន្ធនឹងការដាក់ទណ្ឌកម្ម

១. សាវតារនៃសេចក្តីណែនាំ



UNCLASSIFIED



May 16, 2022

GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS

The U.S. Department of State, the U.S. Department of the Treasury, and the Federal Bureau of Investigation (FBI) are issuing this advisory for the international community, the private sector, and the public to warn of attempts by Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) information technology (IT) workers to obtain employment while posing as non-North Korean nationals. There are reputational risks and the potential for legal consequences, including sanctions designation under U.S. and United Nations (UN) authorities, for individuals and entities engaged in or supporting DPRK IT worker-related activity and processing related financial transactions.

The DPRK dispatches thousands of highly skilled IT workers around the world to generate revenue that contributes to its weapons of mass destruction (WMD) and ballistic missile programs, in violation of U.S. and UN sanctions. These IT workers take advantage of existing demands for specific IT skills, such as software and mobile application development, to obtain freelance employment contracts from clients around the world, including in North America, Europe, and East Asia. In many cases, DPRK IT workers represent themselves as U.S.-based and/or non-North Korean teleworkers. The workers may further obfuscate their identities and/or location by sub-contracting work to non-North Koreans. Although DPRK IT workers normally engage in IT work distinct from malicious cyber activity, they have used the privileged access gained as contractors to enable the DPRK's malicious cyber intrusions. Additionally, there are likely instances where workers are subjected to forced labor.

This advisory provides detailed information on how DPRK IT workers operate; red flag indicators for companies hiring freelance developers and for freelance and payment platforms to identify DPRK IT workers; and general mitigation measures for companies to better protect against inadvertently hiring or facilitating the operations of DPRK IT workers. An Annex provides additional information on DPRK IT workers from reports produced by the UN 1718 Sanctions Committee's DPRK Panel of Experts. The FBI encourages U.S. companies to report suspicious activities, including any suspected DPRK IT worker activities, to local field offices.

UNCLASSIFIED



FACT SHEET: GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS

May 16, 2022

The U.S. Government is issuing this [advisory](#) as a comprehensive resource for the international community, the private sector, and the public to better understand and guard against inadvertent recruitment, hiring, and facilitation of Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) information technology (IT) workers. The advisory provides detailed information on how DPRK IT workers operate and identifies red flag indicators and due diligence measures to help companies avoid hiring DPRK freelance developers and to help freelance and digital payment platforms identify DPRK IT workers abusing their services. Hiring or supporting the activities of DPRK IT workers poses many risks, ranging from theft of intellectual property, data, and funds to reputational harm and legal consequences, including sanctions under both U.S. and United Nations (UN) authorities.

The DPRK has dispatched thousands of highly skilled IT workers around the world, earning revenue for the DPRK that contributes to its weapons programs in violation of U.S. and UN sanctions. These workers:

- Abuse the entire ecosystem of freelance work platforms to surreptitiously obtain IT development contracts from client companies around the world—as well as abuse many social media platforms—to communicate with clients and payment platforms to receive payment for their work;
- Develop applications and software spanning a range of sectors, including, but not limited to, business, cryptocurrency, health and fitness, social networking, sports, entertainment, and lifestyle;
- In many cases misrepresent themselves as foreign (non-North Korean) or U.S.-based teleworkers, including by using virtual private networks (VPNs), virtual private servers (VPSs), purchased third-country IP addresses, proxy accounts, and falsified or stolen identification documents; and
- Use privileged access gained as contractors for illicit purposes, including enabling malicious cyber intrusions by other DPRK actors.

Some red flag indicators of potential DPRK IT worker activity include:

- Multiple logins into one account from various IP addresses in a relatively short period of time, especially if the IP addresses are associated with different countries;
- Frequent transfers of money through payment platforms, especially to People's Republic of China (PRC)-based bank accounts, or requests for payment in cryptocurrency;
- Inconsistencies in name spelling, nationality, claimed work location, contact information, educational history, work history, and other details across a developer's freelance platform profiles, social media profiles, external portfolio websites, payment platform profiles, and assessed location and hours; and
- Inability to conduct business during required business hours, and inability to reach the worker in a timely manner, especially through "instant" communication methods.

ក្រសួងការបរទេសសហរដ្ឋអាមេរិក
 ក្រសួងរតនាគារសហរដ្ឋអាមេរិក និង
 ការិយាល័យស្រាវជ្រាវសហព័ន្ធ (FBI)
 បានចេញសេចក្តីណែនាំនេះ
 នៅថ្ងៃទី១៦ ខែឧសភា ឆ្នាំ២០២២
 សម្រាប់សហគមន៍អន្តរជាតិ វិស័យឯកជន
 និងសាធារណៈជន បន្ថែមការប្រុងប្រយ័ត្ន
 ជាមួយបុគ្គល ឬក្រុមហ៊ុនផ្នែកខាងវិស័យ
 បច្ចេកវិទ្យាព័ត៌មាន (IT) របស់សាធារណរដ្ឋ
 ប្រជាធិបតេយ្យប្រជាមានិតកូរ៉េ



១. សាវតារនៃសេចក្តីណែនាំ (ត)

ក្រុមអ្នកជំនាញ The Panel បានធ្វើការរាយការណ៍លើកដំបូងនៅក្នុងឆ្នាំ២០១៩-២០២០ និងឆ្នាំ២០២១ ពាក់ព័ន្ធជាមួយនឹង បញ្ហាកូរ៉េខាងជើងបានបញ្ជូនអ្នកជំនាញផ្នែកបច្ចេកវិទ្យាព័ត៌មាន (IT) មានជំនាញខ្ពស់រាប់ពាន់នាក់ទៅជុំវិញពិភពលោក

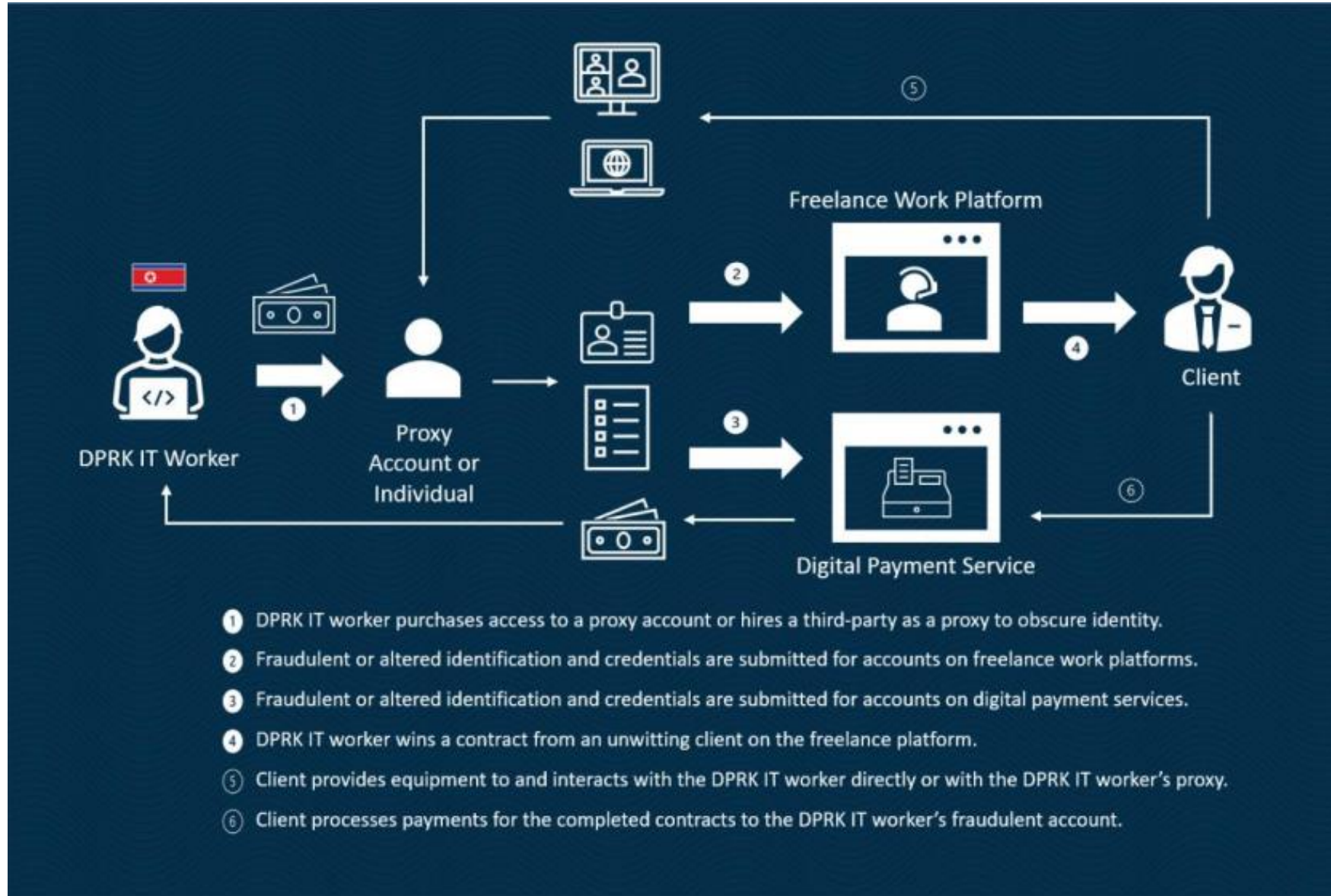
ការជួល ឬគាំទ្រសកម្មភាពរបស់បុគ្គល ឬក្រុមហ៊ុនផ្នែកខាងវិស័យបច្ចេកវិទ្យាព័ត៌មាន (IT) របស់កូរ៉េខាងជើង បង្កហានិភ័យ ជាច្រើន ដូចជា ការលួចកម្មសិទ្ធិបញ្ញា ទិន្នន័យ និងមូលនិធិ រហូតដល់ការប៉ះពាល់ដល់កេរ្តិ៍ឈ្មោះក្រុមហ៊ុនដែលពាក់ព័ន្ធ និង ការដាក់ទណ្ឌកម្ម របស់សហរដ្ឋអាមេរិក និងអង្គការសហប្រជាជាតិ (UN)

ក្នុងករណីជាច្រើនអ្នកជំនាញផ្នែក (IT) របស់កូរ៉េខាងជើង បានបន្តខ្លួនជាអ្នកជំនាញផ្នែកទូរគមនាគមន៍ ដែលមានមូលដ្ឋាន នៅសហរដ្ឋអាមេរិក និង/ឬមិនមែនកូរ៉េខាងជើង

២. គោលបំណងនៃសេចក្តីណែនាំ



៣. ប្រតិបត្តិការរបស់បុគ្គលិក IT នៃកូរ៉េខាងជើង





៣. ប្រតិបត្តិការរបស់បុគ្គលិក IT នៃកូរ៉េខាងជើង (ត)

១. បុគ្គលិក IT របស់កូរ៉េខាងជើង នៅក្រៅប្រទេសមានទីតាំងចម្បងនៅក្នុងសាធារណៈរដ្ឋប្រជាមានិតចិន និងប្រទេសរុស្ស៊ី
២. រកប្រាក់ចំណូលបានច្រើនជាង ៣០០,០០០ដុល្លារ/ឆ្នាំ និងច្រើនជាង ៣ លានដុល្លារ/ឆ្នាំ បើធ្វើការជាក្រុម
៣. កូរ៉េខាងជើងបានកាត់ប្រាក់ចំណូលរហូតដល់ទៅ ៩០ភាគរយ នៃប្រាក់ឈ្នួលរបស់កម្មករនៅក្រៅប្រទេស ដើម្បីបង្កើតប្រាក់ចំណូលប្រចាំឆ្នាំចូលរដ្ឋាភិបាលកូរ៉េខាងជើង ដើម្បីបង្កើតប្រាក់ចំណូលដែលរួមចំណែកដល់កម្មវិធីអាវុធប្រល័យលោក (WMD) និងកម្មវិធីមីស៊ីលផ្លោង បានរាប់រយលានដុល្លារ
៤. កូរ៉េខាងជើងបានបញ្ជូនបុគ្គលិក IT ពីស្ថាប័នសំខាន់ៗ ដូចជា៖
 - នាយកដ្ឋានឧស្សាហកម្មគ្រាប់បែក (MID)
 - ក្រសួងឧស្សាហកម្មថាមពលអាតូមិក
 - ក្រសួងការពារជាតិ និងកងទ័ពប្រជាជនកូរ៉េ
 - ការិយាល័យពាណិជ្ជកម្មបរទេសរបស់គណៈកម្មការអប់រំកូរ៉េខាងជើង និងការិយាល័យបច្ចេកវិទ្យាព័ត៌មាន ទីក្រុងព្យុងយ៉ាង នៃគណៈកម្មាធិការកណ្តាលនៃនាយកដ្ឋានវិទ្យាសាស្ត្រ និងអប់រំ។



៣. ប្រតិបត្តិការរបស់បុគ្គលិក IT នៃកូរ៉េខាងលើ (ត)

ក្រុមហ៊ុន និងបុគ្គលិក IT របស់កូរ៉េខាងលើ បានបន្តខ្លួនទៅធ្វើការនៅតាមតំបន់សំខាន់ៗជុំវិញពិភពលោក ក្នុងប្រតិបត្តិការដូចជា៖ (១). ការបង្កើតកម្មវិធីទូរស័ព្ទដៃ (២). អភិវឌ្ឍន៍កម្មវិធីកម្ចាត់វីរុស (៣). កម្មវិធីប្តូររូបិយប័ណ្ណអេឡិចត្រូនិច (៤). កម្មវិធីល្បែងអនឡាញ (៥). និងកម្មវិធីហ្គេមតាមទូរស័ព្ទ។





៤. សូចនាករទង់ក្រហម Red Flag Indicators

សូចនាករ (Red Flags Indicators) មួយចំនួននៃសកម្មភាពអ្នកជំនាញផ្នែកបច្ចេកវិទ្យាព័ត៌មាន (IT) របស់កូរ៉េខាងជើងដែលក្រុមហ៊ុន ឬស្ថាប័នពាក់ព័ន្ធគួរសម្គាល់ រួមមាន៖

១. ការបើកចូលគណនីតែមួយ ញឹកញាប់ ពីអាសយដ្ឋាន IP ផ្សេងៗ ក្នុងរយៈពេលខ្លី
២. ការផ្ទេរប្រាក់ញឹកញាប់តាមរយៈប្រព័ន្ធទូទាត់ប្រាក់ (Online Payment) ជាពិសេសទៅកាន់គណនីធនាគារនៅសាធារណរដ្ឋប្រជាមានិតចិន (PRC) ឬការទាមទារឱ្យទូទាត់ជារូបិយប័ណ្ណគ្រីបតូ (Crypto Currency)
៣. ភាពមិនប្រក្រតីនៃអក្ខរាវិទ្ធផ្សេងៗ៖ សញ្ញាតិ ទីតាំងការងារ និងព័ត៌មានទាក់ទងប្រវត្តិអប់រំ ប្រវត្តិការងារ និងព័ត៌មានលម្អិតផ្សេងៗទៀត
៤. ភាពមិនប្រក្រតីក្នុងការធ្វើអាជីវកម្មក្នុងអំឡុងពេលម៉ោងការងាររដ្ឋបាល និងឆ្លើយតបក្នុងលក្ខណៈមិនទាន់ពេលវេលា។

៥. ផលប៉ះពាល់ក្នុងការចូលរួមពាក់ព័ន្ធនឹងការដាក់ទណ្ឌកម្ម



១. ក្រុមប្រឹក្សាសន្តិសុខអង្គការសហប្រជាជាតិលេខ ២៣២១ ២៣៧១ និង ២៣៩៧ នឹងចាត់វិធានការផ្លូវច្បាប់ រួមមានការទទួលបានការហាមឃាត់ ឬការដាក់ទណ្ឌកម្ម ចំពោះបុគ្គល ឬអង្គការដែលចូលរួម ឬគាំទ្រសកម្មភាពទាក់ទងនឹងបុគ្គលិក IT របស់កូរ៉េខាងជើង រួមទាំងដំណើរការប្រតិបត្តិការហិរញ្ញវត្ថុដែលពាក់ព័ន្ធ។



២. The Department of the Treasury's Office of Foreign Assets Control (OFAC) មានសិទ្ធិអំណាចក្នុងការដាក់ទណ្ឌកម្មហិរញ្ញវត្ថុលើបុគ្គលណាម្នាក់ ឬដាក់ចូលបញ្ជីខ្មៅ ដោយកំណត់ដូចខាងក្រោម៖

- ចូលរួមសកម្មភាពរបស់រដ្ឋាភិបាល ឬគណបក្សពលករកូរ៉េខាងជើង ដែលបំផ្លាញសន្តិសុខអន្តរជាតិតាមអ៊ីនធឺណិត
- លក់ ផ្គត់ផ្គង់ ផ្ទេរ ឬទិញ ដោយផ្ទាល់ ឬប្រយោល ជាមួយកូរ៉េខាងជើង ឬបុគ្គលណាម្នាក់ដែលធ្វើសកម្មភាពសម្រាប់រដ្ឋាភិបាលនៃគណបក្សពលករកូរ៉េខាងជើង
- ជំនួយជាសម្ភារៈ ឧបត្ថម្ភ ឬផ្តល់ជំនួយផ្នែកហិរញ្ញវត្ថុ ឬបច្ចេកវិទ្យា ឬសេវាកម្មដល់រដ្ឋាភិបាល ឬគណបក្សពលករកូរ៉េខាងជើង

ស្រួចអន្តោល!

