Dear Colleague:

The DPRK continues to support the development of its WMD and missile programs by obfuscating the movement of hundreds of millions of dollars of stolen cryptocurrency through virtual asset service providers (VASPs) such as cryptocurrency exchanges, bridges, mixers and other related blockchain-enabled platforms around the world. In 2023 alone, according to blockchain analysis firm Chainalysis, the DPRK stole an estimated 1 billion USD in virtual assets to fund its weapons of mass destruction and missile programs. DPRK actors are increasingly reliant on exploitation of VASPs, including mixers, bridges, centralized exchanges, and decentralized platforms to steal and launder funds for these illicit programs. Significant effort and coordination on behalf of the blockchain industry and government regulators is needed to further hinder DPRK revenue generation involving virtual assets while preserving legitimate industry operations.

The United States Department of State and the Republic of Korea's Ministry of Foreign Affairs are pleased to invite you to participate in a symposium hosted in New York City on August 27, 2024, from 09:00 – 16:30 (UTC-04:00). The event, which is titled "*Protecting the Virtual Asset Industry from DPRK Exploitation and Disrupting DPRK Revenue Generation: A Joint U.S.-ROK Symposium*," will include presentations aimed at strengthening the ability of VASPs and regulators to identify, disrupt, and report entities and transactions with potential links to DPRK actors, improving VA theft incident response through industry and law enforcement coordination, and enhancing public-private information sharing on DPRK proliferation finance typologies.

The events will be conducted in English, however interpretation into other languages may be available depending on participant need. For attendees unable to travel, a virtual attendance option will be available. If you or your colleagues are interested in attending this event in person or virtually, please sign up using the following link: https://insights.crdfglobal.org/symposium-in-nyc

We kindly request that you **register by July 31, 2024**. Thank you for your consideration.

Sincerely,

Lee Jun-il
Lee Jun-il
Director-General for Korean Peninsula Policy
ROK Ministry of Foreign Affairs

Jung Pak
Dr. Jung Pak
Senior Official for the DPRK
U.S. Department of State

Protecting the Virtual Asset Industry from DPRK Exploitation and

Disrupting DPRK Revenue Generation: A Joint U.S.-ROK Symposium

Proposed Date: August 27, 2024

Location: New York City, USA

DRAFT AGENDA

0830-0900: Registration and Coffee

0900-0915: Opening Remarks

0915-0935: DPRK Virtual Asset (VA) Thefts: Funding the Development of WMD

Objective: Build the connection between DPRK VA theft/laundering and its development of WMD and ballistic missiles. Reinforce the severity of the DPRK threat facing VA industry stakeholders.

0935-1035: Analytic Panel on Case Studies of DPRK Cryptocurrency Heists, Laundering, and Liquidation

Objective: Provide overview through illustrative case studies of the tactics, techniques, and procedures (TTPs) the DPRK uses during each phase of a VA heist: 1) cyber intrusion/initial theft, 2) laundering, and 3) cashout.

Private Sector Blockchain Tracing Expert

1035-1045: Coffee Break

1045-1115: DPRK Virtual Asset Cashout Tactics and Risks to VASPs and Financial Institutions

Objective: Detail how DPRK actors exchange laundered VA for fiat currency and the related sanction/reputational risks DPRK VA cashout presents to centralized VASPs and financial institutions.

Global Centralized Exchange Representative

U.S. or ROK Government Representative

1115-1145: Strengthening Cyber Defenses Against DPRK Intrusions and Thefts

Objective: Provide an update on the TTPs DPRK cyber actors use to compromise VASPs, discuss recent DPRK cyber operations targeting VASPs, and reiterate the importance of blockchain companies 1) integrating cybersecurity principles into their platforms from the beginning, 2) practicing good cyber hygiene, and 3) developing cyber incident response plans.

U.S. / ROK Government Cyber Expert

Global DeFi Platform Representative

1145-1300: Lunch

1300-1345: Law Enforcement Panel and Q+A on Disrupting DPRK VA Laundering

Objective: Explain how law enforcement approaches DPRK VA theft/laundering cases (general focus on the use of civil seizure/forfeiture actions vs. criminal indictments) and encourage private sector cooperation with law enforcement requests.

U.S. Law Enforcement Representative

ROK Law Enforcement Representative

Global Virtual Asset Industry Representative

1345-1430: Regulatory Panel and Q+A on Sanctions and DPRK VA Revenue Generation

Objective: Explain the role supervision/financial sector regulation can play in incentivizing industry to implement strong AML/CFT/CPF protocols; reinforce the importance of transaction monitoring; highlight consequences of non-compliance.

U.S. Regulatory Representative

ROK Regulatory Representative

Global Virtual Asset Industry Representative

1430-1445: Coffee Break

1445 -1600: Industry Panel and Q+A on Successes, Challenges, and Innovations in Identifying and Preventing DPRK VA Laundering

Objective: Provide industry leaders with a platform to describe 1) the challenges they face in identifying and mitigating DPRK VA heists, 2) successful collaborations with others in industry and governments in disrupting VA laundering, and 3) how industry and government can work more effectively together moving forward.

U.S. Virtual Asset Industry Representatives

ROK Virtual Asset Industry Representatives

Global Virtual Asset Industry Representatives

1600-1615: Opportunities for Future Engagement and Assistance

U.S. Government Representative

ROK Government Representative

Objective: Explain capacity building and other resources that are available to support industry and government stakeholders in confronting DPRK VA heists and laundering activities.

1615-1630: Closing Remarks

INVITATION TO JOINT U.S.-ROK INDUSTRY/GOVERNMENT OUTREACH EVENT ON DPRK CRYPTOCURRENCY LAUNDERING

Potential Invitation List:

G7+: UK, Australia, Canada, New Zealand, Japan, Italy, France, Germany, Switzerland, European Union

ASEAN: Singapore, Vietnam, Cambodia, Philippines, Indonesia, Malaysia, Thailand, Laos

U.S. and ROK Counter-DPRK VA Laundering Priority Jurisdictions for Engagement: Seychelles, British Virgin Islands

FATF List of Jurisdictions with Materially Significant VASP Sectors: Argentina, Austria, Bahamas, Belgium, Brazil, Cayman Islands, Cyprus, Denmark, Estonia, Finland, Gibraltar, Greece, Iceland, India, Ireland, Kazakhstan, Lithuania, Luxembourg, Malta, Mexico, Netherlands, Nigeria, Norway, Poland, Portugal, South Africa, Spain, Sweden, Switzerland, Türkiye, Ukraine, UAE

Demarche Text:

-- The United States and the Republic of Korea (ROK) are pleased to invite your government and relevant private sector representatives from your jurisdiction to attend a symposium on preventing DPRK revenue generation involving virtual assets and protecting the virtual asset industry from DPRK exploitation. The DPRK continues to support the development of its WMD and missile programs by obfuscating the movement of hundreds of millions of dollars of stolen cryptocurrency through virtual asset service providers (VASPs) such as cryptocurrency exchanges, bridges, mixers and other related blockchain-enabled platforms around the world.

-- The DPRK is increasingly reliant on virtual assets to support its WMD and ballistic missile programs. In 2023, DPRK stole over 1 billion USD in virtual assets, according to blockchain analysis firm Chainalysis. The blockchain ecosystem provides the DPRK with significant opportunities to evade international sanctions in which the regime hides the proceeds from cyber-enabled thefts of cryptocurrency through complex blockchain laundering processes, complicating efforts by law enforcement to recover stolen funds for return to victims.

-- Given growing concerns about the revenue generated by the DPRK's cryptocurrency heists, the Governments of the United States and the Republic of Korea have released several public alerts about the DPRK cyber threats to the cryptocurrency industry, including in July 2023 (https://www.mofa.go.kr/eng/brd/m_25525/view.do?seq=3&page=1), in April 2022 (https://www.cisa.gov/uscert/ncas/alerts/aa22-108a), and in February 2021 (https://www.cisa.gov/uscert/ncas/alerts/aa21-048a). The Financial Action Task Force (FATF) has published material on red flag indicators of money laundering using virtual assets

(https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html).

-- The private sector has a vital role to play in improving cybersecurity, customer due diligence, and transaction monitoring processes to ensure their services are not exploited by DPRK actors to steal and launder cryptocurrency. Due to the speed with which the DPRK often moves virtual assets under its control and the complexity of DPRK laundering tactics, effective cooperation between industry and law enforcement is critical to tracing and seizing stolen funds for return to victims.

-- In addition to the challenges faced by the private sector, many governments do not yet have the authorities, regulations, or capacity to effectively monitor, regulate, and prevent VASPs operating in their jurisdictions from facilitating DPRK laundering activities. Regulators and law enforcement need the capacity to identify, disrupt, and report entities and transactions with potential links to DPRK actors, invest in public-private information sharing on proliferation finance typologies, and responsibly respond to virtual asset heists impacting their jurisdiction.

-- To improve governmental and private sector capabilities to protect VASPs from and effectively mitigate DPRK virtual asset exploitation, we are planning to hold a symposium on August 27, 2024 , in New York City. This event, which is titled "*Protecting the Virtual Asset Industry from DPRK Exploitation and Disrupting DPRK Revenue Generation: A Joint U.S.-ROK Symposium*" will provide an overview of the threat posed by DPRK illicit cryptocurrency activities, case studies on recent DPRK cryptocurrency heists, and guidance on implementing due diligence and virtual asset recovery. The event will be convened in New York City from 09:00 – 16:30 UTC+09:00. (Note: the event will be conducted in English, however interpretation may be available depending on participant needs.)

-- Venue space is limited so we may not be able to accommodate every request to attend the event in-person. For attendees unable to participate in-person, a virtual attendance option will be available, with details forthcoming.

-- If you or your colleagues are interested in attending this event, in-person or remotely, please sign up by accessing the following link:

https://insights.crdfglobal.org/symposium-in-nyc

-- In order to raise awareness of this issue and the potential risks involved – and further restrict the DPRK's capabilities to exploit the cryptocurrency industry – we would be grateful if you could share this invitation letter with relevant stakeholders in your jurisdiction. Ideal private sector participants could include representatives of cryptocurrency exchanges, blockchain-enabled gaming companies, bridges, mixers, tumblers, and decentralized finance platforms.

-- We thank you for your continued cooperation on this important matter and we appreciate your thoughts on ways to complement or build on this effort.