Joint Statement on Cryptocurrency Thefts by the Democratic People's Republic of Korea and Public-Private Collaboration

The United States, Japan, and the Republic of Korea join together to provide a new warning to the blockchain technology industry regarding the ongoing targeting and compromise of a range of entities across the globe by Democratic People's Republic of Korea (DPRK) cyber actors. The DPRK's cyber program threatens our three countries and the broader international community and, in particular, poses a significant threat to the integrity and stability of the international financial system. Our three governments strive together to prevent thefts, including from private industry, by the DPRK and to recover stolen funds with the ultimate goal of denying the DPRK illicit revenue for its unlawful weapons of mass destruction and ballistic missile programs.

The advanced persistent threat groups affiliated with the DPRK, including the Lazarus Group, which was designated by the relevant authorities of our three countries, continue to demonstrate a pattern of malicious behavior in cyberspace by conducting numerous cybercrime campaigns to steal cryptocurrency and targeting exchanges, digital asset custodians, and individual users. In 2024 alone, our governments have individually and jointly attributed multiple thefts, denominated in virtual asset value in U.S. dollars, to the DPRK: DMM Bitcoin for $308 million, Upbit for $50 million, and Rain Management for $16.13 million. The United States and Republic of Korea additionally attribute to the DPRK, based on detailed industry analysis, thefts last year against WazirX for $235 million and Radiant Capital for $50 million.

As recently as September 2024, the United States government observed aggressive targeting of the cryptocurrency industry by the DPRK with well-disguised social engineering attacks that ultimately deploy malware, such as TraderTraitor, AppleJeus and others. The Republic of Korea and Japan have observed similar trends and tactics used by the DPRK.

Additionally, agencies from our governments have published multiple notifications on the DPRK information technology (IT) workers that also present an insider threat to private sector partners: the United States on 16 May 2022 and 16 May 2024, the United States and the Republic of Korea on 18 October 2023, the Republic of Korea on 8 December 2022, and Japan on 26 March 2024. The United States, Japan, and the Republic of Korea advise private sector entities, particularly in blockchain and freelance work industries, to thoroughly review these advisories and announcements to better inform cyber threat mitigation measures and mitigate the risk of inadvertently hiring DPRK IT workers.

Deeper collaboration among the public and private sectors of the three countries is essential to proactively disrupt these malicious actors' cybercrime operations, protect private business interests, and secure the international financial system. Cooperative public-private efforts in the United States through the Illicit Virtual Asset Notification (IVAN) information sharing partnership, the Cryptoasset and Blockchain Information Sharing and Analysis Center (Crypto-ISAC), and the Security Alliance (SEAL) are examples of newly established mechanisms to facilitate information sharing and incident response. The Republic of Korea and the United States also co-host a series of public-private symposiums to strengthen coordination between the government and private sector in disrupting the DPRK's illicit revenue generation, including on 17 November 2022, 24 May 2023, and 27 August 2024. In Japan, the Financial Services Agency, in collaboration with the Japan Virtual and Crypto Assets Exchange Association (JVCEA), warned relevant businesses about the risk of crypto-asset thefts and requested self-inspections on 26 September and 24 December 2024.

The United States, Japan, and the Republic of Korea will continue to work together to counter the DPRK's malicious cyber activities and illicit revenue generation, including by imposing sanctions on DPRK cyber actors and collaborating to improve cybersecurity capacity across the Indo-Pacific region. The United States, Japan, and the Republic of Korea reaffirm their commitment to combatting cyber threats posed by the DPRK and enhancing their coordination through the trilateral working groups.