United States Senate

COMMITTEE ON BANKING, HOUSING, AND
URBAN AFFAIRS

WASHINGTON, DC 20510–6075

May 19, 2025

The Honorable Scott Bessent
Secretary of the Treasury
U.S. Department of the Treasury
1500 Pennsylvania Ave NW
Washington, DC 20220

The Honorable Pamela Bondi
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530

Dear Secretary Bessent and Attorney General Bondi:

On February 21, 2025, the Lazarus Group, a hacker syndicate backed by the Democratic
People's Republic of Korea (North Korea), stole approximately $1.5 billion in digital currency
from Bybit, a popular cryptocurrency exchange.[1] In the wake of this attack—the "largest crypto
theft of all time"[2]—we write to request information regarding your efforts to combat increasingly
aggressive and frequent cyber-attacks by ransomware groups based in North Korea.

North Korea relies on cryptocurrency theft to subvert U.S.-led international sanctions and to
undermine the security of the United States and our Indo-Pacific allies. The Annual Threat
Assessment of the U.S. Intelligence Community for 2025 states that "North Korea is funding its
military development—allowing it to pose greater risks to the United States—and economic
initiatives by stealing hundreds of millions of dollars per year in cryptocurrency from the United
States and other victims."[3] Between 2017 and 2023, North Korea stole an estimated $3 billion in
crypto hacks, laundering tokens through crypto mixers to effectively mask their origins before
funneling the proceeds back to Pyongyang.[4] These stolen assets have helped keep the regime

---

[1] Federal Bureau of Investigation, "Public Service Announcement: North Korea Responsible for $1.5 Billion Bybit
Hack," February 26, 2025, https://www.ic3.gov/PSA/2025/PSA250226.
[2] CoinDesk, "North Korean Hackers Were Behind Crypto's Largest 'Theft of All Time,'" Aoyon Ashraf, February
21, 2025, https://www.coindesk.com/markets/2025/02/21/north-korean-hackers-were-behind-crypto-s-largest-left-
of-all-time.
[3] Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community,"
p. 28, March 2025, https://www.odni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.
[4] TRM, "Inside North Korea's Crypto Heists: $200M in Crypto Stolen in 2023; Over $2B in the Last Five Years,"
August 18, 2023, https://www.trmlabs.com/post/inside-north-koreas-crypto-heists, CoinDesk, "North Korean
Crypto Hackers Have Stolen $3B Since 2017, Says UN Security Council: Report," Jamie Crawley, March 21, 2024,

afloat and supported continued investments in its nuclear and conventional weapons programs.[5] Reports suggest there are potentially thousands of North Korean-affiliated crypto hackers around the globe.

In recent years, North Korean hackers have shifted from simplistic crypto theft schemes to more sophisticated tactics. Typically, these attacks center around variations of social engineering schemes, designed to exploit vulnerabilities in tech and crypto companies.[6] Hackers have increasingly found ways to infiltrate crypto firms, often faking credentials, resumes, and documents and disguising themselves as American or foreign nationals eligible for work.[7] According to reports, "[t]hey have pretended to be Canadian IT workers, government officials and freelance Japanese blockchain developers. They will conduct video interviews to get a job, or …masquerade as potential employers."[8] In addition, hackers have relied on "phishing and supply chain attacks, and…infrastructure hacks which involve private key or seed phrase compromises."[9]

The Bybit hack reflects a further escalation in North Korea's ability to execute complex crypto theft schemes. In the attack, hackers pulled approximately $1.5 billion from a "cold" crypto storage wallet—a "piece of hardware…kept mostly isolated from online networks" that, prior to the attack, were "considered to be almost impervious to attacks."[10] According to experts, the attack suggests that "North Korea has either expanded its money laundering infrastructure or that underground financial networks, particularly in China, have enhanced their capacity to absorb and process illicit funds."[11] The hack is expected to have significant impacts on the crypto industry and leaves companies scrambling to bolster cybersecurity. Specifically, "staving off North Korean thefts will likely require much higher spending by crypto exchanges."[12]

https://www.coindesk.com/policy/2024/03/21/north-korean-crypto-hackers-have-stolen-3b-since-2017-says-un-security-council-report/; Center for Strategic & International Studies, "Cryptocurrencies and U.S. Sanctions Evasion: Implications for Russia," William Alan Reinsch and Andrea Leonard Palazzi, December 20, 2022, https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia.

[5] Id; Wired, "North Korean IT Workers Are Being Exposed on a Massive Scale," Matt Burgess, May 14, 2025, https://www.wired.com/story/north-korean-it-worker-scams-exposed/.

[6] CoinDesk, "How North Korea Infiltrated the Crypto Industry," Sam Kessler, October 2, 2024, https://www.coindesk.com/tech/2024/10/02/how-north-korea-infiltrated-the-crypto-industry/.

[7] Id.

[8] Wall Street Journal, "How North Korea's Hacker Army Stole $3 Billion in Crypto, Funding Nuclear Program," Robert McMillan and Dustin Volz June 11, 2023, https://www.wsj.com/articles/how-north-koreas-hacker-army-stole-3-billion-in-crypto-funding-nuclear-program-d6fe8782.

[9] TRM, "Inside North Korea's Crypto Heists: $200M in Crypto Stolen in 2023; Over $2B in the Last Five Years," August 18, 2023, https://www.trmlabs.com/post/inside-north-koreas-crypto-heists.

[10] Bloomberg, "North Korea's $1.5 Billion Heist Puts the Crypto World on Notice," February 28, 2025, https://www.bloomberg.com/news/articles/2025-02-28/lazarus-1-5-billion-hack-on-bybit-shakes-up-the-crypto-world-eth?embedded-checkout=true.
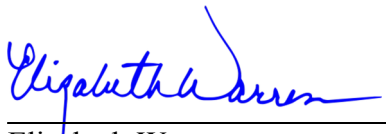
[11] TRM, "The Bybit Hack: Following North Korea's Largest Exploit," February 27, 2025, https://www.trmlabs.com/post/the-bybit-hack-following-north-koreas-largest-exploit.

[12] Bloomberg, "North Korea's $1.5 Billion Heist Puts the Crypto World on Notice," February 28, 2025, https://www.bloomberg.com/news/articles/2025-02-28/lazarus-1-5-billion-hack-on-bybit-shakes-up-the-crypto-world-eth?embedded-checkout=true.
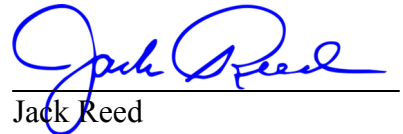
In the wake of the Bybit hack, it is essential that the United States redouble its efforts to prevent North Korean crypto theft. To better understand the scope of North Korea's reliance on the theft of crypto to evade sanctions and finance its weapons programs and the steps the administration is taking to address this urgent national security concern, we ask that you respond to the following questions by June 2, 2025:

1. Please describe the steps your agency is taking to address threats to U.S. national security posed by North Korea's theft of cryptocurrency to earn revenue and bypass sanctions.

2. What additional steps, if any, does your agency plan to take in the wake of the Bybit attack to bolster efforts to prevent North Korean cryptocurrency theft?

3. What are the biggest challenges your agency faces in combatting North Korean cryptocurrency theft? What steps can Congress take to bolster and support enforcement efforts to prevent future crypto theft?

Sincerely,

Elizabeth Warren
Ranking Member
Committee on Banking,
Housing, and Urban Affairs

Jack Reed
United States Senator