

United States Senate

WASHINGTON, DC 20510

August 3, 2023

The Honorable Brian E. Nelson
Under Secretary for Terrorism and Financial
Intelligence
U.S. Department of the Treasury
1500 Pennsylvania Avenue NW
Washington D.C., 20220

Jake Sullivan
National Security Advisor
The White House
1600 Pennsylvania Avenue NW
Washington, D.C. 20500

Dear Under Secretary Nelson and Mr. Sullivan:

We write to express concern about the national security threat posed by North Korea's reliance on digital assets to circumvent international sanctions and embargoes and fund its illegal weapons programs. According to recent comments by White House Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, "[a]bout half of North Korea's missile program has been funded by cyberattacks and cryptocurrency theft," and the country's misuse of these tactics is increasing.¹ Given the pressing nature of this threat, we ask the Administration to provide details on its plan to stop North Korea and its "digital bank-robbing army" from using digital assets "to evade harsh sanctions and support its ambitions to project geopolitical power through nuclear weapons and ballistic missiles."²

The Treasury Department (Treasury),³ Department of Justice (DOJ),⁴ and other national security experts have long noted North Korea's dependence on cryptocurrency. A 2019 United Nations report found that in 2016, North Korea exhibited a "clear shift" to attacking cryptocurrency exchanges for the purposes of "generating financial revenue."⁵ These "large-

¹ CNN Politics, "Half of North Korean missile program funded by cyberattacks and crypto theft, White House says," Sean Lyngaas, May 10, 2023, <https://www.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks/index.html>

² 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>

³ U.S. Department of the Treasury, "Illicit Finance Risk Assessment of Decentralized Finance," April 6, 2023, p. 24, <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>; U.S. Department of the Treasury, "Action Plan to Address Illicit Financing Risks of Digital Assets," September 12, 2022, p. 3, <https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf>

⁴ U.S. Department of Justice, "The Role of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets," September 6, 2022, p. 7, <https://www.justice.gov/ag/page/file/1535236/download>; U.S. Department of Justice, "United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied To Hacks of Two Exchanges by North Korean Actors," press release, August 27, 2020, <https://www.justice.gov/opa/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two-exchanges>

⁵ United Nations Security Council, "Report of the Panel of Experts established pursuant to resolution 1874 (2009)," August 30, 2019, p. 27, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf

scale attacks against cryptocurrency exchanges allow the Democratic People’s Republic of Korea (DPRK) to generate income in ways that are harder to trace and subject to less government oversight and regulation than the traditional banking sector,” enabling North Korean cyber actors, “many operating under the direction of the Reconnaissance General Bureau, [to] raise money for the country’s weapons of mass destruction [programs], with total proceeds to date estimated at up to \$2 billion.”⁶ The United Nations report identified both North Korea’s theft of cryptocurrency through attacks on exchanges and users as well as the mining of cryptocurrency “as a source of funds for a professional branch of the military.”⁷

These reports affirm that “hacking and cybercrime are key to the North Korean regime’s survival” and that the regime is increasingly using crypto to steal and launder illicit funds and finance its weapons program.⁸ Research from blockchain analytics firms shows that of the \$3.8 billion of cryptocurrency stolen last year, \$1.7 billion – about 44 percent – was stolen by North Korea-backed hackers, four times the country’s previous record for crypto theft from 2021.⁹ Over the past five years, North Korea has raised over \$3 billion in crypto heists.¹⁰

A recent *Wall Street Journal* report noted that since 2018, when “North Korea’s digital thieves began hitting their big crypto attacks,” the country’s “missile launch attempts and successes have mushroomed, with more than 42 successes observed in 2022.”¹¹ When asked during a May 2023 hearing of the U.S. Senate Committee on Armed Services about the role that crypto plays in the development of the DPRK’s nuclear arsenal, Lieutenant General Scott Berrier, the Director of the Defense Intelligence Agency, said, “as North Korea steals that money and then tries to turn it into a legal tender, . . . [t]hat is helping them build their nuclear capacity.”¹² Director of National Intelligence Avril Haines added that beyond funding its nuclear program, North Korea’s cyber- and crypto-crime “also pos[es] a cyber-threat to important networks. And that’s part of what it is that we see as a national security threat.”¹³

North Korea has methodically built its expertise in digital assets over the last few years. A 2020 United Nations report found that North Korea hosted an international cryptocurrency conference in 2019 in which “international experts in the Blockchain and Crypto industry gathered in Pyongyang to share their knowledge and vision, established long lasting connections, discussed business opportunities and signed contracts in the field of Information Technology.”¹⁴ One participant was told by the conference organizers that he “should stress the

⁶ *Id.* at p. 4.

⁷ *Id.* at p. 26.

⁸ CNN Politics, “Half of North Korean missile program funded by cyberattacks and crypto theft, White House says,” Sean Lyngaas, May 10, 2023, <https://www.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks/index.html>

⁹ BBC News, “Crypto theft: North Korea-linked hackers stole \$1.7b in 2022,” Kelly Ng, February 2, 2023, <https://www.bbc.com/news/world-asia-64494094>

¹⁰ 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>

¹¹ *Id.*

¹² U.S. Senate Committee on Armed Services, “To receive testimony on worldwide threats,” May 4, 2023, p. 81, https://www.armed-services.senate.gov/imo/media/doc/23-44_05-04-2023.pdf

¹³ *Id.*

¹⁴ United Nations Security Council, “Report of the Panel of Experts established pursuant to

potential money laundering and sanction evasion applications of cryptocurrency and blockchain technology.”¹⁵ Since then, North Korea has succeeded in building “what is essentially a shadow workforce of thousands of IT workers operating out of countries around the world, including Russia and China.”¹⁶ Some of these workers have infiltrated crypto companies by hiring “Western ‘front people’—essentially actors who sit through job interviews to obscure the fact that North Koreans are the ones actually being hired.”¹⁷

That the missile “test buildup by Kim Jong Un’s reclusive regime has occurred at the same time as a concerning upswing in crypto heists”¹⁸ underscores the severity of threat. Treasury must act quickly and decisively to crack down on illicit crypto activity and protect our national security. We therefore request answers to the following questions regarding Treasury’s plans to address the serious national security threats posed by North Korea’s dependence on cryptocurrency no later than August 16, 2023:

1. What steps is the Biden Administration taking to address North Korea’s reliance on cryptocurrency to evade sanctions?
2. Reports indicate that North Korea has stolen \$3 billion in cryptocurrency over the last five years.¹⁹ Does that track with the Administration’s estimates?
3. White House Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger said that over half of North Korea’s missile program has been funded through cryptocurrency and cybercrime, up from a third just a few years ago.²⁰ What is the dollar amount? Does the Administration expect that number to rise?
4. What challenges does the Administration face in arresting North Korea’s growing success in stealing and laundering cryptocurrency and using it to fund its weapons programs? How is it addressing those challenges?
5. What information does the Administration have about which actors are facilitating the exchange of digital assets for other assets, including inputs into its nuclear program?

resolution 1874 (2009),” March 2, 2020, p. 64, https://www.securitycouncilreport.org/atf/cf/%7B65BF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2020_151.pdf

¹⁵ *Id.*

¹⁶ 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>

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.*

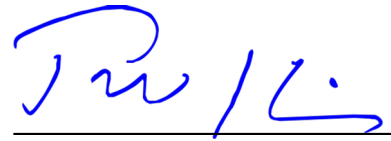
²⁰ *Id.*

Where are these actors based? What actions has the Administration taken against these actors?

Sincerely,



Elizabeth Warren
United States Senator



Tim Kaine
United States Senator



Chris Van Hollen
United States Senator