United States Senate

WASHINGTON, DC 20510

March 8, 2019

The Honorable Michael R. Pompeo
Secretary
U.S. Department of State
2201 C Street, NW
Washington, DC 20520

The Honorable Steven T. Mnuchin
Secretary
U.S. Department of Treasury
1500 Pennsylvania Ave, NW
Washington, DC 20220

Dear Secretary Pompeo and Secretary Mnuchin:

While we support the administration's efforts to seek a pathway for the complete, verifiable, and irreversible denuclearization of North Korea, until such time as it may be appropriate to consider necessary changes to law and statute, we respectfully urge you to fulfill the requirements under U.S. law to impose sanctions against all persons found to have been complicit in North Korea's malicious activities in cyberspace.

On March 3, 2019, the *New York Times* reported that researchers at the private cybersecurity firm McAfee have uncovered an 18-month long campaign of cyber attacks against U.S. and European targets by individuals associated with the North Korean regime, which "include efforts to hack into banks, utilities and oil and gas companies." The reports noted that these attacks were being conducted as recently as last week, when the second U.S.-North Korea summit between President Trump and North Korean dictator, Kim Jong Un, was occurring.

These reports are extremely alarming and are consistent with the increasing malicious capabilities and malign intent of the North Korean regime to develop effective capabilities in cyberspace that can cause serious damage to the United States and our allies. The U.S. government found North Korea responsible for cyber attacks against Sony Pictures in 2014, the cyber theft of $81 million from the Bank of Bangladesh in 2016, and the WannaCry ransomware in 2017. As stated in the Worldwide Threat Assessment of the U.S. Intelligence Community, released on January 29, 2019: "North Korea poses a significant cyber threat to financial institutions, remains a cyber espionage threat, and retains the ability to conduct disruptive cyber attacks."

We therefore urge the Administration to fully comply with the requirements under Section 209 of the North Korea Sanctions and Policy Enhancement Act (Public Law 114-122) and Section 210 of the Asia Reassurance Initiative Act (Public Law 115-409), which require the designation of any persons that knowingly engages in significant activities undermining cybersecurity through the use of computer networks or systems against foreign persons, governments, or other entities on behalf of the Government of North Korea" and codifies Executive Order 13694 of April 1, 2015, relating to blocking the property of certain persons engaging in significant malicious cyber enabled activities.

We ask you to provide answers to the following questions (in classified form, if appropriate):

1. Was the U.S. government, including the State Department and Treasury, aware of this cyber campaign and if so, for how long? Which specific entities or individuals were engaged in these attacks? How are they tied to the government of North Korea?
2. Can you confirm that the attacks were occurring during the time of the Hanoi summit?
3. Have representatives of the U.S. government formally objected to, or raised, North Korea's behavior in cyberspace directly with the representatives of the government of North Korea? If so, when and what was the response? If not, do you plan to raise it in future meetings?

In addition to addressing North Korea's cybersecurity violations, we also urge to you to maintain focus on a range of other reported violations of the U.S. and the United Nations-mandated sanctions regime, including illicit ship-to-ship transfers of prohibited goods, financial transactions on behalf of the North Korean regime, and Pyongyang's continued human rights abuses.

Thank you in advance for your prompt action and response.

Sincerely,

Cory Gardner
United States Senator

Robert Menendez
United States Senator