RON JOHNSON, WISCONSIN, CHAIRMAN

JOHN McCAIN, ARIZONA
ROB PORTMAN, OHIO
RAND PAUL, KENTUCKY
JAMES LANKFORD, OKLAHOMA
MICHAEL B. ENZI, WYOMING
KELLY AYOTTE, NEW HAMPSHIRE
JONI ERNST, IOWA
BEN SASSE, NEBRASKA

THOMAS R. CARPER, DELAWARE
CLAIRE McCASKILL, MISSOURI
JON TESTER, MONTANA
TAMMY BALDWIN, WISCONSIN
HEIDI HEITKAMP, NORTH DAKOTA
CORY A. BOOKER, NEW JERSEY
GARY C. PETERS, MICHIGAN

CHRISTOPHER R. HIXON, STAFF DIRECTOR
GABRIELLE A. BATKIN, MINORITY STAFF DIRECTOR

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

June 8, 2016

The Honorable Jeh Johnson
Secretary
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Johnson:

In light of recent cyber attacks involving the Society for Worldwide Interbank Financial Telecommunication (SWIFT), I write today to request information regarding the Department of Homeland Security's (DHS) response to these attacks.

In February 2016, an anonymous group of cyber criminals reportedly posed as the Central Bank of Bangladesh and used the SWIFT system to fraudulently transfer $81 million from an account at the Federal Reserve Bank of New York to accounts in the Philippines. According to press reports, these criminals exploited weak cybersecurity protections at the Central Bank of Bangladesh to create fully authenticated transfer orders and then used sophisticated malware to hide evidence of the transactions. Similar attacks using SWIFT codes reportedly occurred several months prior at several other banks in countries such as Vietnam and in Ecuador.

A recent report from the cybersecurity company Symantec suggests the cyber criminals who conducted the attack involving SWIFT, the Central Bank of Bangladesh, and the Federal Reserve Bank of New York may be linked to a group called the Lazarus Group that has previously attacked targets in the United States. According to this report, the malicious code used to hide the evidence of the attack on the Central Bank of Bangladesh had been used previously by the Lazarus Group in an attack of Sony Pictures in 2014.

In addition, the Federal Financial Institutions Examination Council, an interagency body that prescribes uniform principles and standards to promote uniformity in the supervision of financial institutions, recently issued a statement calling on financial institutions to "actively manage the risks associated with interbank messaging and wholesale payment networks" and "conduct ongoing assessments of their ability to mitigate risks related to information security, business continuity, and third-party provider management." The statements comes after the Federal Bureau of Investigation reportedly warned financial institutions in the United States to monitor for signs of cyber attacks after "actors have exploited vulnerabilities in the internal environments of the banks and initiated unauthorized monetary transfers over an international payment messaging system."

Given the importance of SWIFT to the global financial system, these recent attacks raise important questions regarding the security practices of member banks and their ability to prevent future attacks. Congress has a responsibility to continue to strengthen our nation's cybersecurity, including

ensuring that the system used by our banks to engage in cross-border transactions is secure. Only by staying a step ahead of these cyber threats can we ensure the security of our financial system.

To better understand DHS's response to these attacks, I ask that you please provide the following information by June 29, 2016:

1. Has DHS provided assistance to the Federal Reserve Bank of New York or any other entity in response to the attacks on the SWIFT system? If so, please explain.

2. Has DHS reviewed the Symantec report linking the recent attack to the Lazarus Group? If so, please provide DHS's assessment of this report.

3. DHS has the express goal of leading "the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure." This is carried out by a variety of programs at DHS, including the United States Computer Emergency Readiness Team (US-CERT). How does DHS work with the financial services sector to better prepare for and respond to cyber attacks like those on the SWIFT system?

4. Does DHS track cyber attacks on financial institutions in the United States? If so, please describe this process.

5. In 2015, Congress passed the Cybersecurity Act of 2015 to enhance the security of private companies and the federal government, including by better sharing of cyber threat information. How is DHS using the authorities under the Cybersecurity Act of 2015 to help secure companies and organizations like SWIFT?

I also request that you ensure that a briefing is scheduled with my staff regarding these issues. The Committee's minority staff is authorized to conduct this investigation under the authority of Senate Rule XXV and Senate Resolution 73 (114th Congress). [redacted] Thank you for your attention to this matter.

With best personal regards, I am

Sincerely yours,

Tom Carper
Ranking Member

cc: The Honorable Ron Johnson
Chairman