

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

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510-6250

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

June 8, 2016

Jaime Caruana
General Manager
Bank for International Settlements
Centralbahnplatz 2, 4051
Basel, Switzerland

Dear Mr. Caruana:

In light of recent cyber attacks involving the Society for Worldwide Interbank Financial Telecommunication (SWIFT), I write today to request information regarding the Bank for International Settlements' guidance on cybersecurity practices to central banks around the world.

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 banks in other countries such as Vietnam and Ecuador.

The Bank for International Settlements provides policy analysis, banking, and internal support services to central banks and plays an important role in coordinating cybersecurity guidance to central banks in response to these attacks. In a November 2015 report prepared for one of the Bank for International Settlements' standing committees, the authors stated that cyber resilience "can be a decisive factor in the overall resilience of the broader financial system" and that "given the stealthy and sophisticated nature of cyber attacks ... advanced capabilities to extensively monitor for anomalous activities are needed."¹ In addition, Gottfried Leibbrandt, SWIFT's CEO, was reportedly in recent contact with the Bank for International Settlements regarding the inclusion of cybersecurity within global supervisory standards.

As the attacks on the SWIFT system raise important questions about the ability of member banks to prevent future attacks, the U.S. Congress has a responsibility to continue to strengthen cybersecurity in the United States, including ensuring that the system used by our banks to engage in cross-border transactions is secure. International financial institutions, including central banks, also have a responsibility to ensure that they stay one step ahead of cyber threats to protect the security of the global financial system.

¹ "Consultative report: Guidance on cyber resilience for financial market infrastructures," Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions, Bank for International Settlements (Nov. 2015).

Mr. Jaime Caruana
June 8, 2016
Page 2

To better understand the Bank for International Settlements' role in preventing future cyber attacks, I ask that you please provide the following information by June 29, 2016:

1. What are the Bank for International Settlements' protocols and practices for sharing information about cybersecurity threats targeting BIS member central banks?
2. Does the Bank for International Settlements provide any technical, operational, managerial, and procedural support to member central banks related to cybersecurity? If so, please explain.
3. Have member central banks provided comments on the November 2015 report on cyber resiliency? If so, please summarize these comments and describe any further actions the Bank for International Settlements plans to take in response.
4. Does the Bank for International Settlements plan to issue revised cyber security standards to central banks or take any further action in response to the recent attacks involving the SWIFT system?
5. Please describe any additional efforts of the Bank for International Settlements' working groups, including through its standing committees, to address the recent attacks involving the SWIFT system.

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).

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