

Congress of the United States

House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

February 14, 2017

The Honorable Eddie Bernice Johnson
Ranking Member
Committee on Science, Space, and Technology
394 Ford House Office Building
Washington, DC 20515

The Honorable Dan Lipinski
Member
Committee on Science, Space, and Technology
394 Ford House Office Building
Washington, DC 20515

The Honorable Don Beyer
Member
Committee on Science, Space, and Technology
394 Ford House Office Building
Washington, DC 20515

Dear Ranking Member Johnson, Rep. Lipinski and Rep. Beyer:

We received and read with interest your letter dated February 9, 2017 related to the Committee's oversight of federal cybersecurity issues. Be assured that our interest in cybersecurity issues is undiminished. We remain committed to ensuring that all federal agencies implement and follow strong cybersecurity protocols. As the new administration, a mere 25 days old, completes its transition and the Senate confirms the President's nominees to lead agencies, the Committee will monitor and work with new administration and agency officials to gather information and ensure that all appropriate policies are followed.

We were pleasantly surprised to learn of your newfound interest in the Committee's oversight and investigatory responsibilities, particularly given your often heated rhetoric attacking the Majority's cybersecurity investigations in the past. This included statements that you were "outraged that the Chairman is recklessly abusing the Committee's investigatory

powers”¹ and that “[t]his is a wasteful use of taxpayer dollars by Chairman Smith and the Science Committee Republicans.”² We trust that your calls last week for oversight of cybersecurity issues are sincere and not, as you state in your letter, the result of “the change of party in the Executive Branch.”³ Your participation in, and assistance with, the next steps in the following ongoing Committee efforts would be welcome:

- The Committee commenced an investigation into the FDIC’s cybersecurity posture upon the receipt of several notifications of major breaches at the FDIC.⁴ The Committee’s investigation identified cybersecurity weaknesses widespread within the FDIC’s information technology infrastructure, culminating in at least 14 major incidents that have been reported to the Committee since February 2016. The Committee also uncovered the existence of a significant attack on the FDIC’s systems sponsored by the Chinese military, dating back to 2010. The Committee also brought to light FDIC leadership’s reticence to reporting breaches to Congress and its willingness to insert countless delays into the agency’s data breach management processes to avoid reporting breaches to Congress in a timely manner. To ensure they do not occur again, these systemic problems with FDIC IT management may require changes in management and policy at FDIC as well as continued Committee oversight; we welcome your assistance in promoting all necessary changes.
- Pursuant to the Committee’s jurisdiction over the National Institute of Standards and Technology (NIST), which is responsible for updating and promulgating standards used to safeguard federal information systems, the Committee is conducting an investigation into the security of former Secretary Clinton’s private email and server arrangement. The Committee found that, indeed, former Secretary Clinton’s private server was subject to attempted attacks by multiple foreign entities, including hackers associated with China, Germany, and Korea.⁵ Despite the issuance of a subpoena, one of former Secretary Clinton’s IT contractors has refused to provide documents and communications crucial to the

¹ Press Release, Hon. Eddie Bernice Johnson, Ranking Member Johnson’s Response to Issuance of Subpoenas in Investigation into Clinton Email Server (Aug. 22, 2016), <http://democrats.science.house.gov/press-release/ranking-member-johnson-response-issuance-subpoenas-investigation-clinton-email-server>.

² Press Release, Hon. Don Beyer, Beyer Denounces Science Committee Republicans’ Clinton Subpoenas (Aug. 22, 2016), <https://beyer.house.gov/news/documentsingle.aspx?DocumentID=407>.

³ Letter from Hon. Eddie Bernice Johnson, Ranking Member, H. Sci., Space, & Tech. Comm., Hon. Don Beyer, and Hon. Dan Lipinski, to Hon. Lamar Smith, Chair, H. Sci., Space, & Tech. Comm. 4 (Feb. 9, 2017).

⁴ See *Interim Staff Report: The Science, Space, and Technology Committee’s Investigation of FDIC’s Cybersecurity* (July 12, 2016), available at <https://science.house.gov/sites/republicans.science.house.gov/files/documents/Final%20GOP%20Interim%20Staff%20Report%207-12-16.pdf>.

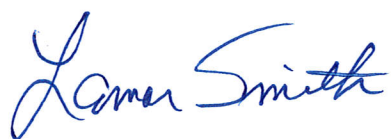
⁵ See *Clinton Server Hack Attempts Came from China, Korea, Germany*, CHICAGO TRIBUNE (Oct. 8, 2016), <http://www.chicagotribune.com/news/nationworld/politics/ct-clinton-emails-hack-20151007-story.html>; Press Release, H. Sci., Space, & Tech. Comm., Smith Statement on FBI’s Reopening of Clinton Email Investigation (Oct. 28, 2016), <https://science.house.gov/news/press-releases/smith-statement-fbi-s-reopening-clinton-email-investigation>.

Committee's investigation. We are sure that you agree that the refusal to comply with a lawfully issued subpoena demands the Committee's continued attention. We look forward to working with you to uphold Congress' oversight prerogatives.

- The Committee commenced oversight of the Federal Reserve Board's cybersecurity posture after press reports indicated that the Federal Reserve had detected more than 50 cybersecurity breaches between 2011 and 2015, which included hacks, acts of espionage, and instances of unauthorized access. Pursuant to its jurisdiction under FISMA and attendant OMB guidelines, the Committee sought information about incident reports logged by the National Incident Response Team, or NIRT, and how the unit responded to and prevented threats from compromising the Federal Reserve's systems. Additionally, the Committee began oversight of a cyberattack at the Federal Reserve Bank of New York in which approximately \$101 million was stolen from the Bank of Bangladesh through compromising the SWIFT Alliance Access server software with malware. Since the NY FED is a global monitor of the SWIFT system, the Committee requested information about the NY Fed's cybersecurity oversight of SWIFT as it related to the Bangladesh heist, and cybersecurity weaknesses in the system at large. While the Committee has received some of the material it has requested and reviewed more *in camera*, responsive items remain outstanding and we welcome your assistance in obtaining and reviewing this information.

Thank you again for your letter and for your offer to join the Majority in its oversight efforts. Please do not hesitate to contact us at any time to discuss these or other issues. In the meantime, Committee Majority staff will reach out to your offices to discuss next steps.

Sincerely,



Lamar Smith
Chair
Committee on Science, Space,
and Technology