LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

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

June 3, 2016

The Honorable Janet L. Yellen
Chair
Board of Governors of the Federal Reserve System
1800 K Street NW
Washington, DC 20006

Dear Ms. Yellen,

The Committee on Science, Space, and Technology is conducting oversight of recent cybersecurity events at the U.S. Federal Reserve. According to recent media reports, the Federal Reserve detected more than 50 cyber breaches between 2011 and 2015, including several incidents involving hackers, as well as other breaches described by Federal Reserve officials as "espionage."[1] According to reports, these security incidents involved hackers who used malicious code or software, individuals who had unauthorized access into the Federal Reserve's systems, information disclosure, inappropriate usage, and fraud. These reports raise serious concerns about the Federal Reserve's cybersecurity posture, including its ability to prevent threats from compromising highly sensitive financial information housed on the agency's systems. To assist in the Committee's oversight of these incidents, we are writing to request a briefing and information related to these security incidents.

According to a *Reuters* report published this week, the Federal Reserve experienced at least 50 breaches of its information technology systems during 2011 through 2015.[2] Of the over 50 breaches identified by the Federal Reserve's National Incident Response Team (NIRT), a team of cybersecurity experts based in New Jersey, reports indicate that Federal Reserve officials suspected hackers or spies to be responsible for multiple incidents.[3] NIRT, which created the incident reports *Reuters* obtained through a Freedom of Information Act (FOIA) request, however, do not indicate whether sensitive information was obtained or whether hackers stole money.[4] Also troublesome is the fact that of the 310 reports provided by the Federal Reserve in response to the FOIA request, hacking attempts were cited in 140 reports and four hacking incidents in 2012 alone were considered acts of "espionage."[5] According to reports, the incidents involving acts of "espionage," could not only refer to threats from foreign governments, but also spying by private individuals or companies.[6]

---

[1] Jason Lange & Dustin Volz, *Fed Reords Show Dozens of Cybersecurity Breaches*, REUTERS, Jun. 1, 2016, *available at* http://www.reuters.com/article/us-usa-fed-cyber-idUSKCN0YN4AM (last visited Jun. 3, 2016).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*

NIRT, which handles higher impact cases involving Federal Reserve breaches, is charged with spearheading the response to security incidents, as well as overseeing the Federal Reserve's cybersecurity posture.[7] Regarded as the "first line of defense for the central banking system," one former NIRT member stated that: "If there's a breach of Fedwire or another critical system, they're going to wake the [Federal Reserve] chairman up out of bed. . . . Anything that compromises the faith and trust in the [government-backed] money system."[8] Given the especially sensitive data stored on the Federal Reserve's systems, which could be extremely valuable in the hands of foreign governments and those who seek to threaten the stability of the U.S. financial system, the Committee is interested in learning how NIRT responds to security incidents, and how the group works to prevent threats from compromising information contained on the Federal Reserve's systems.

The Federal Information Security Modernization Act of 2014 (FISMA) directs Executive Branch departments and agencies to report "major" security incidents to Congress within seven days.[9] The Office of Management and Budget (OMB) released guidelines on October 30, 2015 to assist with determining whether an incident should be classified as a "major" security breach. Because of the reporting requirement contained within FISMA and supplemented by OMB guidelines, the Committee is interested in learning additional information about the details surrounding these reported security incidents at the Federal Reserve, as well as whether the agency has experienced any additional breaches that rise to the level of "major," triggering the congressional reporting requirement.

To assist in the Committee's oversight of the Federal Reserve's cybersecurity posture and its response to the security incidents, please contact Committee staff by June 10, 2016 to arrange a briefing on the matter. Please also provide the following documents and information as soon as possible, but by no later than noon on June 17, 2016. Unless otherwise noted, please provide the requested information in unredacted format for the time frame from January 1, 2009 to the present:

1. All cybersecurity incident reports created by NIRT and local cybersecurity teams.

2. A detailed description of all confirmed cybersecurity incidents.

3. All documents and communications referring or relating to higher impact cases handled by NIRT or local cybersecurity teams.

4. All documents and communications relating to NIRT's policies and procedures for responding to cybersecurity incidents, including the incident guide.

---

[7] Shane Harris, *Exclusive: Meet the Fed's First Line of Defense Against Cyber Attacks*, FOREIGN POLICY, Apr. 29, 2014, *available at* http://foreignpolicy.com/2014/04/29/exclusive-meet-the-feds-first-line-of-defense-against-cyber-attacks/ (last visited Jun. 3, 2016).

[8] *Id.*

[9] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283.

5. An organizational chart for the Office of the Chief Information Officer, the Office of the Chief Information Security Officer, and NIRT.

The Committee on Science, Space, and Technology has jurisdiction over the National Institute of Standards and Technology which develops cybersecurity standards and guidelines to support the implementation of and compliance with FISMA as set forth in House Rule X.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format. An attachment provides information regarding producing documents to the Committee.

If you have any questions about this request, please contact Lamar Echols or Caroline Ingram at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

Barry Loudermilk
Chairman
Subcommittee on Oversight

cc: Mr. Mark Bialek, Inspector General, Board of Governors of the Federal Reserve System and Consumer Financial Protection Bureau

The Honorable Eddie Bernice Johnson, Ranking Minority Member

The Honorable Don Beyer, Ranking Member, Subcommittee on Oversight

Enclosure

Responding to Committee Document Requests

1. In complying with this request, you are required to produce all responsive documents, in unredacted form, that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to the Committee.

2. In the event that any entity, organization or individual denoted in this request has been, or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.

3. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, or thumb drive) in lieu of paper productions.

4. Documents produced in electronic format should also be organized, identified, and indexed electronically.

5. Electronic document productions should be prepared according to the following standards:

   (a) The production should consist of single page Tagged Image File ("TIF"), or PDF files.

   (b) Document numbers in the load file should match document Bates numbers and TIF or PDF file names.

   (c) If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.

6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.

7. Documents produced in response to this request shall be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.

8. When you produce documents, you should identify the paragraph in the Committee's schedule to which the documents respond.

9. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.

10. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with the Committee staff to determine the appropriate format in which to produce the information.

11. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.

12. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.

13. In complying with this request, be apprised that the U.S. House of Representatives and the Committee on Science, Space, and Technology do not recognize: any of the purported non-disclosure privileges associated with the common law including, but not limited to, the deliberative process privilege, the attorney-client privilege, and attorney work product protections; any purported privileges or protections from disclosure under the Freedom of Information Act; or any purported contractual privileges, such as non-disclosure agreements.

14. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.

15. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, you are required to produce all documents which would be responsive as if the date or other descriptive detail were correct.

16. Unless otherwise specified, the time period covered by this request is from January 1, 2009 to the present.

17. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.

18. All documents shall be Bates-stamped sequentially and produced sequentially.

19. Two sets of documents shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 324 of the Ford House Office Building.

20. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive

documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Schedule Definitions

1. The term "document" means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.

2. The term "communication" means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email (desktop or mobile device), text message, instant message, MMS or SMS message, regular mail, telexes, releases, or otherwise.

3. The terms "and" and "or" shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.

4. The terms "person" or "persons" mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.

5. The term "identify," when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.

6. The term "referring or relating," with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.