

# 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](http://www.science.house.gov)

May 24, 2016

The Honorable Martin J. Gruenberg  
Chairman  
Federal Deposit Insurance Corporation  
550 17th Street NW  
Washington, DC 20429

Dear Mr. Gruenberg,

The Committee on Science, Space, and Technology is continuing its oversight of recent security events at the Federal Deposit Insurance Corporation (FDIC).<sup>1</sup> Following the Committee's May 12, 2016 hearing, during which representatives from the FDIC testified,<sup>2</sup> additional information has come to light regarding the effectiveness of the agency's cybersecurity measures, attempts to circumvent providing full and complete responses to the Committee's requests, and concerns that the agency may attempt to take retaliatory action against whistleblowers. Because of this new information, the Committee is writing to request additional documents and transcribed interviews with key individuals who have played a role in managing the agency's cybersecurity initiatives, as well as individuals who have been involved with the agency's production of requested materials to the Committee.

In recent weeks, the Committee has learned additional information about significant shortfalls in the agency's cybersecurity practices intended to guard against data security breaches. Although the FDIC's Chief Information Officer and Chief Privacy Officer, Lawrence Gross, testified at the hearing that the "FDIC has a strong information security program to identify events that could signal a data security incident,"<sup>3</sup> the Committee has obtained information in contradiction of this statement. Mr. Gross' testimony was a misrepresentation, at best, of the strength of the agency's cybersecurity posture.

While all of the cybersecurity incidents reported to Congress in the last three months have involved departing employees, Mr. Gross represented during the hearing that this fact was simply a coincidence.<sup>4</sup> In reality, however, the FDIC apparently has not focused its

---

<sup>1</sup> Letter from Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech., to Hon. Martin Gruenberg, Chairman, Fed. Deposit Insurance Corp. (Apr. 8, 2016); Letter from Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech., to Hon. Martin Gruenberg, Chairman, Fed. Deposit Insurance Corp. (Apr. 20, 2016).

<sup>2</sup> H. Comm. on Science, Space, & Tech., *FDIC Data Breaches: Can Americans Trust that Their Private Banking Information is Secure?*, 114<sup>th</sup> Cong. (May 12, 2016) [hereinafter FDIC Hearing, May 12, 2016].

<sup>3</sup> See Statement of Lawrence Gross, Chief Information Officer, Fed. Deposit Insurance Corp. (May 12, 2016), at 5 (emphasis added).

<sup>4</sup> FDIC Hearing, May 12, 2016, *supra* note 2, at 40, 58.

cybersecurity efforts on monitoring current employees' computer activity, including whether current employees are downloading sensitive information on to portable storage devices. Although the FDIC monitors departing employees' computer activity, it has apparently opted to forego taking a close look at the computer activity of individuals who remain employed at the agency. This leaves important information, including personally identifiable banking information for millions of Americans and banks' living wills, vulnerable to data breaches by FDIC employees, who currently have access to sensitive information at the agency.

Additionally, while the Committee applauds the success of the FDIC's Data Loss Prevention (DLP) program, which was responsible for catching each of the recent data breaches involving a departing employee, the Committee has since learned that the same program is *incapable* of detecting if an employee copies, downloads, or otherwise transfers encrypted information from FDIC systems. This information raises serious concerns about whether additional data breaches have occurred without detection due to inherent weaknesses in the FDIC's systems used to monitor data breaches. Even more troublesome, the Committee is concerned that Mr. Gross was not forthcoming during his recent testimony about significant information regarding vulnerabilities within the agency's cybersecurity programs.<sup>5</sup>

Regrettably, the FDIC's decision to withhold information pertinent to its cybersecurity posture is yet another example of the agency's continued reticence to being fully transparent with the Committee's investigation. According to information obtained by the Committee, FDIC officials charged with identifying and producing responsive documents to the Committee's requests regarding the recent data breaches have actively worked to limit the scope of the Committee's requests such that the universe of responsive information falls far short of a full and complete production to the Committee. In fact, during the hearing, Members of the Committee questioned Mr. Gross about whether anyone at the agency voiced any concern regarding the manner, scope, or methods the agency employed to identify and gather responsive documents.<sup>6</sup> Although Mr. Gross both denied that the agency limited the scope of the Committee's requests or that anyone at the agency voiced any concerns,<sup>7</sup> information obtained by the Committee raises questions about the veracity of Mr. Gross' testimony. So that the Committee can determine whether the FDIC improperly limited the scope of the Committee's requests and whether anyone at the agency raised concerns about how the FDIC determined the scope of the Committee's requests, please produce all documents and communications referring or relating to these matters.

As Committee Members explained during the hearing, the FDIC has repeatedly attempted to shield information from Congress. When providing responses to the Committees' letters, the FDIC initially produced documents redacted extensively for information the agency deemed to be "confidential." Despite the agency's inability to cite statutory authority or a valid privilege for redacting information, the agency resisted the Committee's request for providing unredacted documents until faced with the threat of the Committee's use of the compulsory process to obtain

---

<sup>5</sup> Letter from Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech., to Hon. Martin Gruenberg, Chairman, Fed. Deposit Insurance Corp. (May 19, 2016).

<sup>6</sup> FDIC Hearing, May 12, 2016, *supra* note 2, at 28–29.

<sup>7</sup> *Id.*

unredacted documents. These redactions included the name of the employee responsible for the October 2015 security breach in Florida. Ironically, this employee was the same individual the Committee found, in fact, to have received a Master of Information Technology Management, despite Mr. Gross' testimony that she was not proficient with using computers.<sup>8</sup> As an agency that has faced a seemingly never ending series of security breaches, it should focus its resources first and foremost on reforming its internal cybersecurity mechanisms, instead of endeavoring to conceal information from the Committee.

Additionally, according to information obtained by the Committee, agency personnel have reportedly instructed FDIC employees to avoid placing things in writing, including information related to the agency's data breaches. If true, these allegations raise serious concerns about whether the agency is attempting to circumvent federal records requirements, diminish the universe of information that could be responsive to congressional requests, and ultimately hide the truth from congressional overseers.

In light of the serious nature of these allegations, I request that all documents responsive or related to the Committee's requests and communications between and among employees of the FDIC referring or relating to the Committee's requests, be preserved. So that a full and complete record of documents may be provided to the Committee in response to future document requests that the Committee may deem appropriate, please:

1. Preserve all e-mail, electronic documents, handwritten documents, and data created since January 1, 2009, concerning the FDIC's cybersecurity posture, including any and all information related to data breaches.

For the purpose of this request, "preserve" means taking reasonable steps to prevent the partial or full destruction, alteration, testing, deletion, shredding, incineration, wiping, relocation, migration, theft, or mutation of electronic records, as well as negligent or intentional handling that would make such records incomplete or inaccessible.

2. Exercise reasonable efforts to identify and notify former government employees, and any other relevant third party who may have access to such electronic records, that they are to be preserved; and,
3. If it is a routine practice of any agency employee, contractor, or related third party to destroy or otherwise alter such electronic records, either halt such practices or arrange for the preservation of complete and accurate duplicates or copies of such records, suitable for production if requested.

To assist the Committee in answering outstanding questions material to its ongoing investigation, we request that you make the following individuals, listed in no particular order, available for a transcribed interview by Committee staff:

---

<sup>8</sup> *Id.* at 40.

1. Roberta K. McInerney, Deputy General Counsel (Consumer and Legislation)
2. Andy Jiminez, Director, Office of Legislative Affairs
3. Christopher J. Farrow, Special Advisor
4. Cyndi Whitaker-Russell, Special Assistant, Information Security and Privacy Staff
5. Roderick E. Toms, Acting Chief Information Security Officer, Information Security and Privacy Staff
6. John S. Kidd, Deputy Director, Infrastructure Services Branch
7. Richard Lowe, Incident Lead
8. Jay Foltz, Information Technology Specialist
9. Henry Griffin, Assistant General Counsel

Please contact Committee staff by May 31, 2016, to schedule the requested interviews. Additionally, please provide all documents and communications referring or relating to FDIC's response(s) to my letters dated April 8 and 20, 2016, including but not limited to documents showing that employees raised concerns related to the scope of the Committee's requests and how the FDIC determined the scope of the Committee's requests, by June 7, 2016. Further, the Committee anticipates holding an additional hearing on the FDIC's cybersecurity posture. Please ensure you are available to testify at a hearing on July 14, 2016.

Finally, as the Committee continues its investigation, we would like to remind you of the protections for whistleblowers found in the Whistleblower Protection Act (WPA).<sup>9</sup> As you should know, the WPA is a key tool for rooting out wrongdoing and serves as the foundation for delineating rights of whistleblowers. Often, whistleblowers function as the primary means for informing Members of Congress of misconduct within the Executive Branch. Any action taken against whistleblowers not only has a chilling effect on the willingness of federal employees to report waste, fraud, and abuse, but is unlawful. The Committee takes seriously any concerns regarding reprisal against whistleblowers and will investigate accordingly, if allegations are brought to the Committee's attention.

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.

---

<sup>9</sup> 5 U.S.C. § 7211 provides in pertinent part: "The right of employees, individually or collectively, to petition Congress or a Member of Congress, or to furnish information to either House of Congress, or to a committee or Member thereof, may not be interfered with or denied."

The Honorable Martin J. Gruenberg  
May 24, 2016  
Page 5

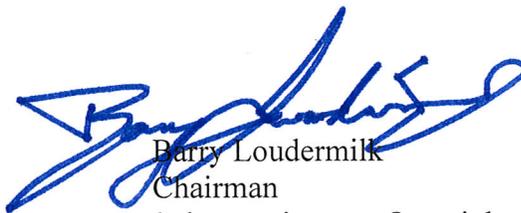
When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format. An 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: 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 October 1, 2015 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.