**INTERIM STAFF REPORT:**
**THE SCIENCE, SPACE, AND TECHNOLOGY**
**COMMITTEE'S INVESTIGATION OF FDIC'S CYBERSECURITY**

**To:** Republican Members, Committee on Science, Space, and Technology

**From:** Majority Staff

**Date:** July 12, 2016

**Re:** Full Committee Hearing: "Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?" (July 14, 2016, at 10:00 a.m.)

---

This interim report provides hearing background for the House Science, Space, and Technology Committee. The Committee is scheduled to hold a hearing on July 14, 2016, to examine the Federal Deposit Insurance Corporation's (FDIC) cybersecurity posture, prior Congressional testimony by FDIC officials, and the agency's response to the Committee's investigation. The hearing witnesses will be FDIC Chairman Martin J. Gruenberg and the Acting Inspector General Fred W. Gibson. This hearing is occurring midway through a lengthy Committee investigation. Staff intends to update this report at the conclusion of the investigation.

## I. Overview of the Committee's Investigation

Pursuant to the Committee's legislative jurisdiction over portions of the Federal Information Security Modernization Act of 2014 (FISMA), the Committee receives an annual FISMA report from each department and agency subject to the statute. FISMA also requires notification to select Congressional Committees, including the Science Committee, whenever an agency experiences a major information technology (IT) security breach. Committee staff reviewing the FDIC's FISMA report noted some anomalies. Then, on February 26, 2016, and March 18, 2016, the Committee received written notification of major breaches. In an effort to better understand the circumstances of these breaches, on April 8, 2016, Chairman Smith sent a letter to FDIC Chairman Gruenberg requesting documents, information, and a briefing from the agency.[1]

On February 26, 2016, Gruenberg wrote Chairman Smith reporting a breach that occurred in Florida on October 15, 2015, and FDIC learned of the breach on October 23, 2015.[2] The FDIC represented in its initial memorandum to the Committee that the separating employee

---

[1] Letter from Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech. to Hon. Martin J. Gruenberg, Chairman, Fed. Deposit Insurance Corp., Apr. 8, 2016 [hereinafter Letter, Apr. 8, 2016].
[2] Letter from Hon. Martin J. Gruenberg, Chairman, Fed. Deposit Insurance Corp., to Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech. (Feb. 26, 2016) [hereinafter Letter, Feb. 26, 2016].

inadvertently "and without malicious intent" downloaded sensitive banking information as well as "customer data for over 10,000 individuals."[3] The employee downloaded the information to a portable storage device referred to as a thumb drive and removed it from the premises. The Committee has since learned FDIC made misrepresentations in its February 26, 2016, notification to the Committee. The FDIC Office of Inspector General (OIG) issued a report on July 8, 2016, which contradicts FDIC's representations to Congress.

According to Chairman Gruenberg's March 18, 2016, notice, a separating employee copied "sensitive FDIC information," which "included customer data for over 44,000 individuals" to a portable storage device.[4] This notice also stated that the "individual inadvertently and without malicious intent" downloaded the information and data.[5] The OIG has since clarified and corrected the record on this particular breach as well. The facts as the Committee now knows them are discussed below.

Shortly after the Committee sent its initial letter, the OIG contacted the Committee relaying information about ongoing audits of the agency's cybersecurity posture as well as raising concerns about other major breaches that the agency failed to report to Congress. The Committee also received credible whistleblower allegations stating that the agency was mischaracterizing the severity of the breaches and intentionally withholding information from Congress related to other major information security breaches. On April 20, 2016, Chairman Smith wrote the FDIC requesting information related to other unreported breaches.[6]

Alarmingly, the IG and several whistleblowers[7] told the Committee that the agency appeared to be withholding documents from the Committee even after twice certifying verbally that they had produced all responsive documents. Allegations of withholding documents led Chairman Smith to send a May 10, 2016, letter to the IG requesting all documents *not* produced by the agency. On May 12, 2016, the Oversight Subcommittee held a hearing on this matter.[8] Witnesses were the Chief Information Officer Lawrence Gross and the IG. At the hearing, Members noted numerous inconsistencies in Gross' testimony. These inconsistencies were outlined in a May 19, 2016, letter to FDIC from Chairman Smith and Subcommittee Chairman Loudermilk. To date, the agency has not provided a substantive response to each of the concerns raised about the veracity of Gross' testimony. Gross' testimony will be discussed in greater detail in Section V, of this report.

---

[3] Letter, Feb. 26, 2016.
[4] Letter from Hon. Martin J. Gruenberg, Chairman, Fed. Deposit Insurance Corp., to Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech. (Mar. 18, 2016) [hereinafter Letter, Mar. 18, 2016].
[5] Letter, Mar. 18, 2016.
[6] Letter from Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech. to Hon. Martin J. Gruenberg, Chairman, Fed. Deposit Insurance Corp., Apr. 20, 2016 [hereinafter Letter, Apr. 20, 2016].
[7] The Chairman received an anonymous letter from a whistleblower on Apr. 25, 2016, raising various concerns related to cybersecurity and the FDIC's cooperation with the Committee's investigation.
[8] *FDIC Data Breaches: Can Americans Trust that Their Private Banking Information Is Secure? Hearing Before H. Comm. on Science, Space, & Tech., Subcommittee on Oversight,* Hearing Transcript, 114th Cong. (May 12, 2016) [hereinafter Hearing, May 12, 2016].

The culmination of the FDIC's discreditable performance at the May 12, 2016, hearing along with their obstruction and concealment of facts and documents, caused Chairmen Smith and Loudermilk to send a May 24, 2016, letter requesting the following:

1) the FDIC Chairman to testify on July 14,

2) requesting additional documents related to FDIC's responses to the Committee,

3) requesting the agency preserve all documents and communications, and

4) requesting transcribed interviews of nine FDIC employees.

As of today's hearing, the Committee has conducted seven transcribed interviews, reviewed approximately 15,000 pages of documents produced by the agency, the IG, and whistleblowers as part of the Committee's ongoing investigation.

## II. Background on the FDIC's Cybersecurity Breaches

In letters dated February 26, 2016, and March 18, 2016, the FDIC notified the Science Committee of two major security incidents.[9] These notifications were required since the incidents met the Office of Management and Budget's (OMB) guidelines for classifying an incident as a "major" security breach.[10]

### *A. September 2015 Data Breach Occurring in New York*

On or about September 29, 2015, the FDIC learned that a poor performing and disgruntled employee in New York returned all electronic devices when she left her job at FDIC, with the exception of a portable USB device containing sensitive resolution plans, commonly known as living wills, sensitive banking information, and the social security numbers of 28,000-30,000 individuals. **This breach was not reported to Congress, but instead simply referenced in the agency's annual FISMA report.** The circumstances of recovering the USB device and the device's especially sensitive contents raise serious questions about why this breach was never separately reported to Congress. Members are advised to question FDIC's witness about the circumstances surrounding this breach.

[9] Letter from Hon. Martin J. Gruenberg, Chairman, Fed. Deposit Insurance Corp., to Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech. (Feb. 26, 2016) [hereinafter Letter, Feb. 26, 2016]; Letter, Mar. 18, 2016, *supra* note 2.

[10] Memorandum from Shaun Donovan, Dir., Office of Management & Budget to Heads of Executive Departments & Agencies, *Fiscal Year 2015-2016 Guidance on Federal Information Security & Privacy Management Requirements* (Oct. 30, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf (last visited Jul. 14, 2016).

## *B. The October 2015 Breach Occurring in Florida*

The security breach reported in the February 26th letter involved an FDIC employee who reportedly copied sensitive personally identifiable information or PII for over 10,000 individuals onto a portable storage device prior to separating from employment at the FDIC.[11] Contrary to FDIC's representation to the Committee, this breach in fact effected "a total of 71,069 individuals and entities (consisting of 40,354 individuals and 30,715 banks and other entities)"[12] In total, the employee stored over 100,000 files on the device. The Committee is very concerned that FDIC knowingly made gross misrepresentations regarding the disparity in the number of effected individuals and entities. In addition, the employee downloaded "Suspicious Activity Reports, Bank Currency Transaction Reports, [Bank Secrecy Act] Customer Data Reports and a small subset of personal work and tax files."[13] On October 15, 2015, the individual officially separated from the FDIC and removed the portable storage device from FDIC premises.[14] Eight days later, the FDIC became aware of the incident and on November 6, 2015, referred the matter to the OIG.[15]

During a briefing for Committee staff on April 21, 2016, FDIC staff made misrepresentations regarding the former employee's intent. Specifically, FDIC staff told Committee staff that the former FDIC employee was simply trying to download family photos when the PII was transferred to the portable storage device. The OIG confirmed this was not the case. In reality, when confronted about taking the data on a portable storage device, the former employee denied owning a portable storage device and claimed she would never do such a thing. During the May 12, 2016, hearing the CIO testified "[T]he individuals involved in these incidents were not computer proficient."[16] To the contrary, the OIG found that the former employee created two folders on the portable storage device, one for a small set of personal files and another folder solely for FDIC materials, with each of the FDIC files conveniently labeled with bank names or the with the types of bank data in the files.[17] This demonstrates an understanding of computers, information downloads, and storage – not the work of a novice computer user.

Furthermore, the Committee later learned that the former employee holds two masters degrees, including one in Information Technology Management.[18] According to the university website describing the Masters in Information Technology program where the employee received her degree, "the master's degree in information technology management focuses on emerging technologies and the management of both IT and people engaged in **computer**

---

[11] Letter, Feb. 26, 2016, *supra* note 7.
[12] Office of the Inspector General, *FDIC's Process for Identifying & Reporting Major Information Security Incidents*, July 8, 2016 [hereinafter OIG Report in re: Congressional Notification].
[13] Aaron Boyd, *FDIC Waited Months to Report Major October Data Breach*, FEDERAL TIMES, Apr. 20, 2016, *available at* http://www.federaltimes.com/story/government/cybersecurity/2016/04/20/fdic-major-breach/83233956/ (last visited Jul. 14, 2016).
[14] Letter, Feb. 26, 2016, *supra* note 7.
[15] OIG Report in re: Congressional Notification.
[16] Letter from Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech. to Hon. Martin J. Gruenberg, Chairman, Fed. Deposit Insurance Corp., May 19, 2016 [hereinafter Letter, May 19, 2016] citing Hearing, May 12.
[17] OIG Report in re: Congressional Notification.
[18] Letter, May 19, 2016.

**technology enterprises**."[19] Mr. Gross' claim that the employee in question was not computer proficient raises serious questions regarding whether his testimony was intentionally misleading.

On November 19, 2015, the FDIC requested the assistance of the OIG because the employee denied possessing the device and on December 2, 2015, refused to meet with FDIC staff with whom she had previously worked.[20] This fact contradicts the FDIC's claim that the employee was non-adversarial and cooperative in recovering the portable storage device. The former employee hired an attorney to engage in a negotiation of return of the portable storage device.[21] After negotiations, the FDIC recovered the device on December 8, 2015.[22] Again, these facts poke holes in the agency's narrative that this was an inadvertent breach.

**This security incident is particularly troublesome given that the FDIC did not ultimately recover the portable storage device from the former employee until nearly two months after the device was removed from FDIC premises.[23] Further, according to information obtained by the Committee, the FDIC did not report the incident to Congress as mandated by FISMA until prompted to do so by the FDIC OIG.** Over four months after the breach, the FDIC wrote to Congress on February 26, 2016, to inform the appropriate congressional committees of the incident, opting to report the breach only after the OIG informed the FDIC that the incident met the OMB's guidelines for classifying an incident as a "major" security breach.[24] The FDIC's apparent hesitation to inform Congress of the security incident not only raises concerns about the agency's willingness to be transparent and forthcoming with Congress, but raises further questions about whether additional information stored in FDIC systems has been compromised without being brought to the attention of Congress, according to federal requirements.

## *C. February 2016 Data Breach Occurring in Texas*

On March 18, 2016, FDIC wrote the Science Committee informing it of a security breach involving an employee who obtained sensitive data for 44,000 individuals prior to separating from employment at the agency.[25] Earlier this year, an FDIC employee who was in the process of separating from agency employment copied personal information onto a personal portable storage device. In the process of loading information onto the storage device, the employee copied sensitive customer data for over 44,000 individuals.[26] When the employee left the FDIC

---

[19] Letter, May 19, 2016, citing Webster University, *Masters in Information Technology Management, available at* http://www.webster.edu/business-and-technology/academics/information-technology-management.html (last visited May 17, 2016) (emphasis added).
[20] OIG Report in re: Congressional Notification at 6-7.
[21] *Id.* at 7.
[22] *Id.* at 7.
[23] *Id.* (emphasis added).
[24] Memorandum from Shaun Donovan, Dir., Office of Management & Budget to Heads of Executive Departments & Agencies, *Fiscal Year 2015-2016 Guidance on Federal Information Security & Privacy Management Requirements* (Oct. 30, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf (last visited Jul. 14, 2016) [hereinafter OMB Memorandum].
[25] Letter, Mar. 18, 2016, *supra* note 2.
[26] *Id.*

on February 26, 2016, the employee took the storage device from the premises.[27] Upon learning of the incident three days later, FDIC personnel worked to recover the device.[28] The device was ultimately recovered on March 1, 2016.[29]

### *D. Retroactively Reported Breaches*

On May 9, 2016, FDIC retroactively reported five additional major breaches to the Committee. In one of those instances, an employee retired from FDIC and took three portable storage devices containing over 49,000 individuals' personal data. In total, over 160,000 individuals have recently been a victim of having their personal information leave the FDIC by "accident." Only after the Oversight Subcommittee's hearing on May 12, 2016, FDIC decided to offer credit monitoring to the individuals whose PII was compromised in the breaches.

### *E. FDIC's Cybersecurity Problems Are Not New*

On May 24, 2013, then FDIC Inspector General Jon T. Rymer sent a memorandum (the 2013 Memo) to FDIC Chairman Gruenberg informing him of a "computer security incident."[30] Among other things, the 2013 Memo found that in October 2010, the FDIC's Division of Information Security learned that "an FDIC employee's desktop computer had been compromised by an advanced persistent threat."[31] The advanced persistent threat in this case is believed to have been the Chinese government. The same threat was able to compromise FDIC computers in 2011, and again in April 2013. In essence, a foreign government penetrated FDIC's computers and the workstations of high-level agency officials, including the former Chairman, the former Chief of Staff, and the former General Counsel of the agency.[32] In all, twelve workstations were compromised and ten FDIC servers were penetrated and infected by a virus created by a hacker.[33] The OIG was particularly critical of the agency for violating its own policies and for failing to alert appropriate authorities.[34] The OIG notified appropriate congressional committees of the breach.[35]

The current CIO Lawrence Gross took over in November 2015, but prior to his permanent status, the agency had several acting CIOs and one other permanent CIO. Witnesses testifying before the Committee as part of this investigation raised concerns about whether the inconsistency in leadership effecting the cybersecurity posture as well as whether the current CIO Mr. Gross is fit to serve in this position. These issues will be discussed in greater detail

---

[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] Memorandum from Jon T. Rymer, Inspector Gen., Fed. Deposit Insurance Corp. to Hon. Martin J. Gruenberg, Chairman, Fed. Deposit Insurance Corp., May 24, 2013 [hereinafter FDIC IG, May 2013 Memo].
[31] *Id.* at 5.
[32] *Id.* at 9.
[33] *Id.* at 10.
[34] *Id.* at 2–3.
[35] *Id.* at 4.

below. The Committee's investigation will continue but at this point we are in a position to release some preliminary findings.

**CURRENT COMMITTEE FINDINGS:**

1. **The Chief Information Officer (CIO) has created a toxic work environment, misled Congress, and retaliated against whistleblowers.**

2. **The FDIC deliberately evaded Congressional oversight.**

3. **The FDIC has historically experienced deficiencies related to its cybersecurity posture and those deficiencies continue to the present.**

# III. The FDIC's Cybersecurity Posture Continues to be Weak

## *A. The Inspector General's Reports Found FDIC Failed to Timely Notify Congress and Other Relevant Agencies of Major Incident(s) and the FDIC Did Not Take Steps to Guard Against Insider Cybersecurity Threats.*

In two reports issued on July 8, 2016, the OIG found the following significant weaknesses in the agency's handling of information security breaches. In addition to the factual misrepresentations the FDIC staff made to the Committee which are discussed in Sections II and V of this interim report, the OIG also found the following:

- Several factors contributed to the September 2015, New York breach in which a disgruntled employee without authorization downloaded sensitive resolution plans, also referred to as living wills. Chief, among the contributing factors, was the agency's failure to implement an insider threat program.[36]

- During 2014 and 2015, the FDIC began to take steps toward establishing a formal insider threat program. These efforts were halted. If such a program were in place, the seven reported breaches could have been prevented or at the very least mitigated.[37]

- The former employee had an extensive history of incidents rising to the level of a security risk, including carrying out a breach several months prior to the September breach where

[36] Office of the Inspector General, *FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans*, July 8, 2016 [hereinafter OIG Report in re: Sensitive Resolution Plans].
[37] *Id.*

the employee transmitted unencrypted, sensitive information to two personal e-mail accounts and later denied that the activity was prohibited.[38]

- In a separate report also released on July 8, 2016, the OIG found that the FDIC's data breach incident policies, procedures, and guidelines did not address major incidents.

- The large volume of potential breaches identified by the data loss prevention tool and the limited number of people review these potential breaches makes it to conduct meaningful analysis of the information.[39]

- FDIC did not properly interpret and apply the criteria for a major incident as articulated in the Office of Management and Budget Memorandum. The OIG found that reasonable grounds existed to deem the Florida breach major and on February 19, 2016, informed FDIC of the same. In fact, the OIG is of the opinion that the "that ground existed to designate the incident as major as of December 2, 2015." The FDIC ultimately reported the incident four months later on February 26, 2016.[40]

- Senior management at the FDIC and individuals within the Chairman's office, including the Deputy to the Chairman, Chief Operating Officer, and Chief of Staff, knew about the incident as early as December 7, 2015, yet opted to report the incident only after the OIG urged the agency of its requirement to report the breach to Congress in accordance with OMB requirements.[41]

- As previously discussed in Section II of this Interim Report, the OIG found that representation made in the congressional notification were "unsupported by adequate evidence and/or inconsistent with information available at the time."[42] In other words, the FDIC made false statements to Congress.

- Between the two reports, the OIG made a total of eleven recommendations all of which the agency agreed with and pledged to implement.

## *B. The Committee's Prior Hearing Revealed FDIC Has Not Taken Steps to Prevent Breaches*

On May 12, 2016, the FDIC Chief Information Officer Lawrence Gross testified that as part of the FDIC's response to the breaches, the agency has taken steps to minimize employees' use of portable storage devices. According to Mr. Gross, however, at the time of the hearing, slightly less than 50 percent of employees could still use portable storage devices.[43] Testimony

[38] *Id.*
[39] OIG Report in re: Congressional Notification at ii.
[40] *Id.* at ii.
[41] *Id.* at 17.
[42] *Id.* at ii.
[43] Hearing, May 12, 2016, *supra* note 6, at 67.

from FDIC staff obtained in June 2016, indicates that employees still have access to portable storage devices, although the percentage of employees outside of the Division of Information Technology remains unclear.[44]

Although the Committee believes that the FDIC should work to limit employees' use of portable storage devices, the FDIC should be working to limit the use immediately. Given that the first breach of which the Committee was notified occurred nine months ago, the Committee remains concerned that the FDIC has still not implemented sufficient precautionary measures to ensure that additional breaches do not occur.

Additionally, during the Committee's May 12, 2016, hearing, Representative Zoe Lofgren asked a series of questions about Digital Rights Management (DRM), software capable of preventing unauthorized distribution of sensitive materials, and whether the program could have prevented the breaches.[45] Specifically, Ms. Lofgren asked Mr. Gross whether the FDIC has implemented DRM and whether the FDIC could be certain that breached materials were not further copied and distributed.[46] Mr. Gross testified that the FDIC *did not* have DRM in place and the only countermeasure the FDIC had in place was a signed affidavit from the former employees, stating that they did not disseminate the information.[47] Regrettably, there was and remains no way for the FDIC to ensure with certainty that the employees did not further disseminate the information.[48]

## C. *The CIO Laptop Initiative is Over Budget and Will Cause More Problems*

Through the Committee's transcribed interviews of individuals within the FDIC Division of Information Technology, the Committee learned that CIO Larry Gross unilaterally decided recently to purchase over 3,300 laptops for use by FDIC employees because of a purported high risk with not having furnished equipment.[49] To garner support for his decision, Mr. Gross convinced FDIC Chairman Martin Gruenberg of the necessity to devote substantial resources, totaling a minimum of $5 million,[50] to purchasing thousands of laptops, arguing that laptops are necessary to strengthen the FDIC's cybersecurity posture to control access to FDIC resources.[51] The former Acting Chief Information Security Officer (CISO) and other employees within the Division of Information Technology strongly disagreed with Mr. Gross' decision to move forward with the laptop initiative, stating that the initiative would in fact present even greater

---

[44] H. Comm. on Science, Space, & Tech., Transcribed Interview of [redacted], at 89-90 (Jun. 28, 2016) hereinafter [redacted] Tr.]
[45] Hearing, May 12, 2016, *supra* note 6, at 46.
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] H. Comm. on Science, Space, & Tech., Transcribed Interview of [redacted], at 14 (Jun. 10, 2016) [hereinafter [redacted] Tr.]; [redacted] Tr., *supra* note 28, at 67.
[50] [redacted] Tr., *supra* note 33, at 13–14; 17.
[51] *Id.* at 12.

security risks, contrary to Mr. Gross' assertion.[52] Mr. Gross, however, chose to ignore experts' advice move forward with implementing the program.

In addition to Mr. Gross' decision to prematurely and unilaterally proceed with the laptop initiative without thoroughly considering experts' advice to the contrary, Mr. Gross is working to expedite the laptop initiative, with an anticipated implementation date of July 31, 2016.[53] Although Mr. Gross' plans to implement the program by the end of July, he has not yet secured the millions of dollars necessary to cover the initiative.[54] Testimony from FDIC staff indicates that Mr. Gross has not only failed to submit a budget request for the laptop initiative, but has also been told by FDIC's Division of Finance that the agency does not have additional funds necessary to cover the project.[55]

According to information obtained by the Committee, Mr. Gross also provided misleading information to his superiors, including Chairman Gruenberg, about the necessity of the laptop initiative.[56] The former Acting CISO testified, **"if the [C]hairman is making decisions based on this type of information—now it's starting to make sense, why this laptop project was greenlighted, certain things were greenlighted, certain artificial schedules were given out, even though there is no chance of these projects being successful."**[57]

## IV. The CIO Has Created a Toxic Work Environment and Concealed Important Information from the FDIC Chairman

**FINDING: The Chief Information Officer (CIO) has created a toxic work environment, misled Congress, and retaliated against whistleblowers.**

Testimony obtained by the Committee shows that CIO Larry Gross has concealed information from FDIC Chairman Martin Gruenberg about the purported success of initiatives for which the CIO advocates as measures to improve the agency's cybersecurity posture. For example, during meetings with the Chairman Gruenberg, Mr. Gross has inflated the potential success of the laptop initiative, as well as the FDIC's efforts to implement Digital Rights Management (DRM).[58] The Special Advisor to the CISO testified:

> **A. My understanding is he [Larry Gross] has told the Chairman things that are not true, as far as the laptops are more secure, DMR [Digital Rights Management] is going fast.**[59]

---

[52] *Id.* at 10.
[53] *Id.* at 80.
[54] [redacted] Tr., *supra* note 28, at 70.
[55] *Id.*
[56] [redacted] Tr., *supra* note 33, at 128–29; [redacted] Tr., *supra* note 28, at 66.
[57] Tr., *supra* note 33, at 129 (emphasis added).
[58] [redacted] Tr., *supra* note 28, at 66.
[59] *Id.* (emphasis added).

Although individuals within the CIO's office have vehemently disagreed with Mr. Gross' characterization of the potential success of the laptop initiative to enhance the agency's cybersecurity, Mr. Gross has not presented Chairman Gruenberg with the full set of facts on the ability of the laptop initiative to improve the agency's cybersecurity. The Special Advisor to the CISO testified:

> Q. So with the laptop rollout, can you just give us a brief explanation of that project?
>
> A. Yes. The laptop project—and I have the documents somewhere, and I will find them and give them to you. **But the laptop project, Larry [Gross] went to the Chairman and said the laptops are more secure than the desktops in our home use through the token. Security disagreed with Larry [Gross], but because the Chairman is hearing one voice—and that is the CIO's voice—he is taking the word of the CIO.**[60]

By presenting Chairman Gruenberg with a limited set of facts surrounding major cybersecurity initiatives, Mr. Gross has silenced and ignored those who disagree with his viewpoints. This has not only led to a toxic work environment where debate is stymied and where individuals fear retaliation for disagreeing with Mr. Gross,[61] but it has deterred experts and long-serving FDIC employees within the Division of Information Technology from weighing in on important decisions.[62]

## *A. The CIO Retaliates Against Those Who Disagree with Him and Others Have Retired Early*

Despite beginning his tenure as CIO in November 2015, just eight months ago, Mr. Gross has created a work environment defined largely by vindictiveness and retaliation, relocating at least one cybersecurity expert to another division of the FDIC, causing cybersecurity experts within the Division of Information Technology to retire prematurely, and retaliating against individuals within the CIO organization who have provided testimony to the Committee during the course of its investigation.

In one case, Mr. Gross removed the former CISO for disagreeing with him about whether the Florida incident should have been reported to Congress. According to testimony obtained by the Committee, the former CISO was adamant that the breach should be reported to Congress according to the requirements outlined in OMB Memorandum 16-03.[63] Mr. Gross, however, disagreed and after some behind the scenes machinations eventually removed the former CISO

---

[60] *Id.* at 67 (emphasis added).
[61] *Id.*at 78–79.
[62] *Id.* at 79.
[63] *Id.* at 51–52.

from his position. In removing him, Mr. Gross instructed him to find a position within another division of the FDIC.[64] The Special Advisor to the CISO testified:

> Q. ... With Mr. Farrow, with Chris Farrow, what is your understanding as to why he left his position?
>
> A. My understanding, things really went downhill after he talked to Mr. Gross about the meeting we had. Also, Chris [Farrow] was adamant that this was—should have been reported, the Florida incident should have been reported [ to Congress]. There were disagreements on the way the DBMT [Data Breach Management Team] was going, that Larry [Gross] wasn't getting back with the DBMT. He wasn't following the rules. **Larry [Gross] does—one thing I know now, Larry does not like you to disagree with him. There are other—another example, somebody disagreed; they're moved out.**
>
> Chris Farrow—I think it was over my Christmas break—was given 4 hours to find another job. **After the OIG [Office of Inspector General] report came out, he was gone within 2 days, moved out, right out from under us. What are my gut feelings? Disagreement over this incident.**[65]

In yet another example of the consequences of the toxic work environment created by Mr. Gross, the former Deputy Director of Infrastructure Services chose to retire early after nine years of working at the FDIC.[66] The former Deputy Director of Infrastructure Services testified that Mr. Gross was focused on his own agenda, creating challenges for the Division of Information Technology, including risk to the agency and an impact to the mission of the agency.[67] The former Deputy Director testified:

> A. When the CIO then started, rather than working with us to understand some of these challenges and where we were, my impression was that he was more focused on his own agenda, which then created a whole other series of challenges for us. And I had become eligible to retire in August of 2015, so what I wanted to do then is I informed by immediate supervisor, which was Russ Pittman, that I will be looking to retire towards the end of April timeframe and hopefully we would be able to have a transition to someone else.
>
> [. . .]

---

[64] *Id.*
[65] *Id.* at 51–52 (emphasis added).
[66] H. Comm. on Science, Space, & Tech., Transcribed Interview of [redacted], at 7 (Jun. 8, 2016).
[67] *Id.* at 11–13.

**And given the combination of the fact that I wasn't feeling like I was being as successful as I could, the frustrations with the budget office, as well as the direction the CIO was taking us, and my own personal issues, I made the decision to retire.**[68]

The former Deputy Director went on to explain that the work environment and actions taken by Mr. Gross as CIO were detrimental to the mission of the agency.[69] He testified:

Q. Do you think these challenges that you're discussing and the reasons that you're leaving the agency, do you think those ultimately have an impact on FDIC's mission?

A. I can't as a fact state that. My impression is, and **I've stated this before, that I do believe that it creates a risk to the agency.** In my opinion, there's nothing definitive, you can't prove, you know that type of a statement. **But the impression I would have is that there is an impact to the mission of the agency by not funding, by not replacing things.**[70]

Finally, the Special Advisor to the CISO testified that, above all, Mr. Gross is "vindictive," retaliating against individuals within the CIO organization possibly solely for their willingness to provide testimony to the Committee.[71] She testified:

**Q. Would you consider the FDIC a hostile workplace because of Mr. Gross?**

**A. Yes.**

Q. Do you feel comfortable disagreeing with him?

A. No.

Q. And why is that?

A. **The man is vindictive. You know, I don't know if it is because Roddy came here and testified—he was one of the nine—the emails he is getting now.** Yesterday—well, Saturday, or it was Sunday, he got an invite from—invite from Larry Gross, and it said: "You have not been answering my emails. We are going to have a meeting tomorrow."

So, I mean, Roddy is really good about answering emails.

---

[68] *Id.* (emphasis added).
[69] *Id.* at 12.
[70] *Id.* (emphasis added).
[71] [redacted] Tr., *supra* note 28, at 78.

So Roddy writes back and said: "Could you tell me what I haven't replied to?"

This morning, that request was off the—Larry just canceled it, but he is bombarding security with email after email.

[. . .]

**I mean, he is just—he is very vindictive. He will take you off of a project if you disagree.** You are no longer project lead, and you find out in front of everybody that you are not the project lead.[72]

Given the toxic work environment created by Mr. Gross, individuals within the CIO organization are rapidly departing. The Special Advisor to the CISO testified:

**A.** **Oh, we are losing people right and left.** John Kidd is resigning. Steve Anderson, the deputy director of our budget and stuff, he is resigning. Mark Felton, acquisitions, he is resigning. Ted Bruce, the contract specialist, because Larry is doing all this stuff with contracts, he is leaving.

Q. **All these people you just named off are leaving directly because of [Larry Gross]--**

A. Yes.

Q. -- Mr. Gross' –

A. And more are talking about leaving.[73]

Equally troubling is that despite Mr. Gross' testimony before the Committee in May 2016, and the Committee's continued investigation into the FDIC's response to the cybersecurity breaches, the hostile work environment created by Mr. Gross is worsening. The Special Advisor to the CISO testified:

**Q.** **Would you say that the work environment—the hostile work environment is getting worse?**

**A.** **Yes.**[74]

---

[72] *Id.* at 78–79 (emphasis added).
[73] *Id.* at 81–82 (emphasis added).
[74] *Id.* at 79 (emphasis added).

# V. The FDIC Purposefully Evaded Congressional Oversight

**FINDING: The FDIC deliberately evaded Congressional oversight.**

Upon learning about the security breaches at the FDIC, the Committee wrote two letters, requesting documents and communications about the incidents.[75] In response to the letters, however, the FDIC opted only to provide a narrow subset of documents, instead of conducting a thorough, good faith search for all responsive materials. Even more troublesome, the FDIC certified to the Committee that it produced all responsive materials. But for assistance from the FDIC OIG, it would not have come to the Committee's attention so quickly – the agency's willful obstruction of the Committee's investigation.

## *A. The FDIC Has a Long Standing History of a Lack of Transparency into Cybersecurity Issues*

**FINDING: The FDIC has historically experienced deficiencies related to its cybersecurity posture and those deficiencies continue to the present.**

As noted above, in 2013, the FDIC OIG issued a report finding that the FDIC computer system – even the former Chairwoman's computer – had been hacked by a foreign government, likely the Chinese.[76] One witness told Committee staff that the former CIO Russ Pittman instructed employees not to discuss or proliferate information about this foreign government penetration of the FDIC's network in order to avoid effecting the outcome of Chairman Gruenberg's confirmation by the U.S. Senate.[77] There was a concern that if news got out about the foreign government hack, Mr. Gruenberg's confirmation to the position of Chairman may be jeopardized.[78] This is one earlier example of the current pattern observed by the Committee of concealing information from Congress. The American people and FDIC employees have a right to know that their PPI and sensitive banking information is being actively protected. Where there are lapses, it is Congress' responsibility to provide the facts surrounding the breach and hold those responsible accountable for the lapse(s).

## *B. FDIC Misrepresented the Nature of the Breaches in a Briefing to Science Committee Staff*

During a bipartisan briefing to Science Committee Staff, held on April 21, 2016, FDIC staff misrepresented the nature of the breaches to staff. FDIC staff explained that in the Florida incident, for example, the former employee was cooperative and non-adversarial and that the breach was non-malicious. According to testimony obtained by the Committee, FDIC staff

[75] Letter, Apr. 8, 2016, *supra* note 1; Letter from Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech., to Hon. Martin Gruenberg, Chairman, Fed. Deposit Insurance Corp. (Apr. 20, 2016).
[76] FDIC IG, May 2013 Memo, *supra* note 21.
[77] [redacted] Tr., *supra* note 28, at 72–73.
[78] *Id.*

thought that Committee staff would buy into the "story" presented by the FDIC. The Special Advisor to the CISO testified:

> Q. You may or may not be aware the Committee requested a briefing back in April 2016 on the reported breaches. In that briefing, a number of FDIC staff characterized the breaches as inadvertent, non-malicious, and the breacher as cooperative. We now know those characterizations are not accurate.
>
> Do you know why the FDIC would intentionally provide inaccurate information to Committee staff?
>
> A. From what Martin [Henning] said to Roddy Toms after the Gross, he said: We had a good story; I don't know what went wrong.
>
> **I think they thought they were getting away with it; that they were going to lie, that the staff—that you guys wouldn't have the documents that you have.**
>
> Q. And so that was Mr. Henning's takeaway from the initial briefing?
>
> A. That was his takeaway after—so he thought he did a great job, because before Martin [Henning] went, I talked to him and I said: "Are you prepared?"
>
> He goes: "Yes."
>
> And I said: "All I am going to tell you is what my daddy always said. Tell the truth.
>
> **Oh yeah, we have a story. He told me that.**
>
> He goes to you guys on the 18th, I think. He comes back: "Oh, it was great, blah, blah, blah."
>
> **See, the FDIC thought it was over then. Nothing else was going to happen.**[79]

Testimony obtained by the Committee shows that FDIC staff created a narrative for the Committee in an effort to deter the Committee from pursuing the issue of the agency's cybersecurity breaches further. Unfortunately, the FDIC's efforts to shield the truth from the Committee at its initial briefing on the matter were the first example in a continued pattern of obstruction and reticence by the FDIC to be fully transparent with the Committee's investigation.

[79] *Id.* at 91–92 (emphasis added).

## C. *FDIC Failed to Produce all Documents and Communications Responsive to the Committee's Request*

On April 22, 2016, the Committee received a production of 118 pages of documents from the FDIC responding to the Committee's initial April 8, 2016, letter. After receiving information from whistleblowers related to an additional unreported breach which occurred in October 2015, the Committee sent another letter dated April 20, 2016, requesting additional documents and testimony. Shortly after receiving the FDIC's production in response to the April 20, 2016, letter, the FDIC OIG contacted Committee staff raising concerns that the agency failed to provide all responsive documents contrary to the instructions provided with every oversight inquiry the Committee sends to federal department and agencies. Likewise, agency whistleblowers told Committee staff that FDIC had not provided a full and complete production.

As previously noted, this was contrary to verbal statements made by FDIC staff during a telephone call on or about May 6, 2016. Twice during the May 6 telephone call, FDIC staff verbally certified that the agency had provided all responsive documents to both of the Committee's letters. This statement turned out to be false. Committee staff, suspecting that FDIC had withheld certain documents from the Committee, separately wrote the OIG on May 10, 2016, requesting the documents withheld by the agency.[80] The OIG prior to the May 12, 2016, hearing produced substantially more documents than the agency. On May 12, 2016, Subcommittee Chairman Loudermilk questioned CIO Gross about the discrepancy:

> **Rep. Loudermilk:** Okay. Thank you. Mr. Gross, what I have here is--this is the stack of documents that the FDIC provided to the Committee in response to our inquiry. This stack of documents, however--I may need a forklift. This stack of documents was provided to the Committee by the Inspector General's Office. Why were these documents not provided to the Committee by the FDIC?
>
> **Mr. Gross**: I had an opportunity to review the material provided by the IG, and in reviewing that material, a lot of it is duplicative, so the material that you received from us with the incident response forms that are in there, it includes information that has been duplicated in the IG's response. The incident response forms provide a summary of the incident, and it's—it may in fact provide a more comprehensive review of each of the incidents more so than what's in the documents. I did note that there were several copies of what we call our Data

[80] Letter from Hon. Lamar Smith, Chairman & Barry Loudermilk, Subcommittee Chairman, H. Comm. on Science, Space, & Tech., to Fred W. Gibson, Acting Inspector General, Fed. Deposit Insurance Corporation. (May 10, 2016) [hereinafter Letter, May 10, 2016].

Breach Management Guide that was included in the material provided by the Inspector General, and there were multiple copies of that. That document is still currently being developed and in review.[81]

[. . .]

**Rep. Loudermilk:** Okay. Okay. But you did say that you had reviewed the materials—

**Mr. Gross:** I did—

**Rep. Loudermilk:** --provided—

**Mr. Gross:** I did a cursory review.[82]

Despite testifying that Mr. Gross had reviewed the materials provided by the OIG and stating that "a lot of it is duplicative," and even giving specific examples of documents he found to be duplicative, Mr. Gross later changed the characterization of his review. When Chairman Loudermilk asked about e-mails withheld from the Committee by FDIC, Mr. Gross shifted his story to say that he had only done a "cursory review" of the materials.[83] **Further, Mr. Gross' contention that the documents provided by OIG are duplicative is not accurate.** The agency only provided the Committee with 88 pages of documents responsive to the Committee's April 20 letter, while the OIG provided 883 individually unique responsive documents. It appears that Mr. Gross only wanted to provide the Committee with testimony that supported his narrative and was prepared to only discuss examples that were cherry picked from the OIG's document production.

Chairman Loudermilk also raised concerns about FDIC's apparent attempts to limit the scope of the Committee's document request. Mr. Gross had the following exchange with Chairman Loudermilk:

**Rep. Loudermilk:** To your knowledge, was anyone in your office or the legal division directed to limit the response to the Committee's request?

**Mr. Gross:** I'm not aware of anyone making such a statement or providing any such direction.[84]

Witnesses appearing before the Committee for interviews stated just the opposite. Witnesses testified that FDIC intentionally limited the scope of the documents provided to the Committee. One current FDIC employee with knowledge of the manner in which FDIC undertook its

[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] *Id.*

response to the Committee testified that "normally when there is a congressional request, the right group of litigation counsel would get together with whatever division is substantively responsible. If it is in the supervision area, it might be in the supervision division, that sort of thing, and assess where records might be."[85] In marked contrast, the following occurred in response to the Science Committee's requests:

> In this case, the Office of Legislative Affairs called a meeting, or a conference call, on April 11th to assess how to respond. And then subsequent, the second -- a similar kind of thing in response to the second letter.[86]
>
> ***
>
> We -- the calls were coordinated by, and lead by the Office of Legislative Affairs. In the first one, we and legal were in my office on speakerphone. And we had litigation counsel who would typically be involved. We had Michael Saulnier, S-a-u-l-n-i-e-r, who is the tech guy who would do the email search. And we had Matt Kepniss and myself. Was there anybody else? Yeah, two litigation branch counsel, Michael Saulnier, Matt Kepniss and myself. And on the line besides the Office of Legislative Affairs, a couple of people. There was Rick Lowe of the CISO staff. I think it was only Rick Lowe, L-o-w-e. And when there was a description of what the product -- there is a multipart request, but the main part of it, I would say, is when Rick Lowe described the incident risk analysis documentation that they have. [redacted] **indicated that that was what we would respond with [the Incident Reports only].** Let's make sure that that living -- referred to as living document is fully updated, and not part of the request that happens with what we respond with.[87]

The FDIC's Office of Legislative Affairs (OLA), specifically [redacted], the OLA Director decided to depart from the normal course of action when responding to a Congressional request. In fact, he directed staff to provide a limited response. The witness, a current FDIC employee, told Committee staff that the General Counsel's office offered a litigation branch counsel to do a full and complete search, but "[redacted] indicated that the IRA [Incident Report Analysis] would suffice for current purposes."[88] Mr. [redacted], according to the witness, unilaterally decided to limit documents produced to the Committee. Specifically, he declined the Office of General Counsel's (OGC) offers to assist in searching for communications related to cybersecurity incidents.

The Committee provides extremely detailed instructions on responding to its oversight requests. Mr. [redacted]' actions are in direct contradiction to those instructions and may rise to the

---

[85] H. Comm. on Science, Space, & Tech., Transcribed Interview of [redacted], at 68 (Jun. 21, 2016) [hereinafter [redacted] Tr.].
[86] *Id.* at 69.
[87] *Id.* (emphasis added).
[88] *Id.* at 70.

level of obstruction of a Congressional investigation. Another effort by FDIC to avoid transparency has come to light over the course of the Committee's investigation. On at least one occasion, FDIC Deputy General Counsel [redacted] instructed FDIC staff *not* to put opinions related to what is a major cybersecurity breach in writing – seemingly in an effort to avoid Congressional oversight. The following section discusses this opaque practice at FDIC.

## *D. [redacted], the FDIC's Deputy General Counsel Instructed Certain Employees Not to Put Opinions Related to Cybersecurity Breaches in Writing*

Committee staff learned from whistleblowers that FDIC Deputy General Counsel [redacted] directed staff on more than one occasion not to place certain opinions and analysis related to major cybersecurity breaches in writing. A current FDIC employee in the OGC had the following exchange during a transcribed interview:

> Q. Did you have a conversation with anyone about not putting things in records -- in emails?
>
> A Well, at a certain point the deputy general counsel, [redacted], had told me and one or two others, I believe, in the opinions unit [not to put things in emails]. I don't recall who was on the phone at what time, but said the direction as I recall, it was relating to interpretation of major [cybersecurity] incident.[89]

[redacted] deliberately tried to prevent FDIC attorneys from creating records that would be responsive to the Committee's request in this investigation. Witnesses also said she based this directive on the sensitive nature of the subject matter and the fact that high-ranking agency officials were involved in the decision-making. The current FDIC OGC employee testified again that [redacted] cautioned against putting information regarding major cybersecurity breaches in writing:

> Q. So just to clarify, on -- you said that [redacted] told you -- did she tell you to tell other people or she just told you not to put things in writing?
>
> A. **She told us not to put anything in writing on that subject [of cybersecurity breaches].**[90]

[redacted] order caused inefficiencies and consternation. The current FDIC OGC attorney appearing before the Committee relayed that the directive created a "difficult situation." Specifically, he stated:

---

[89] *Id.* at 13.
[90] *Id.* (emphasis added).

Q. Did you find it difficult to do your job or did you find it difficult to do your job as an attorney if you are not able it to put things in writing?

A. I found that a difficult situation.[91]

There are indications in the record that [redacted] has in the past issued a similar directive not to put opinions and analysis in writing. Documents provided to the Committee show that this culture of concealment may extend as far back as the Oversight and Government Reform Committee's investigation of Operation Chokepoint.[92] Below is a document memorializing one current FDIC staffers concern that after Operation Chokepoint, the OGC is obfuscating their opinions and facts related to FDIC's actions to determine whether a breach is a major incident under FISMA and the OMB guidance interpreting the statute.

[Page Intentionally Left Blank]

[91] *Id.* at 19.

[92] Operation Choke Point was a federal initiative forcing banks to terminate relationships with businesses deemed "high-risk" by federal regulators. The U.S. Department of Justice and the FDIC were partners in this initiative. *See generally* H. Comm. on Oversight and Gov't Ref. Staff Report, "Federal Deposit Insurance Corporation's Involvement in "Operation Choke Point," Dec. 8, 2014.

**From:** [redacted]
**Sent:** Friday, April 22, 2016 2:31 PM
**To:** [redacted]
**Subject:** MFR 22 Apr 2016 -FW: FISMA 2014 Data Breach 30 Day Not
**Importance:** High

There appears to be some hang-ups within Legal ... finding ways to postpone Congressional notifications

After Matt received my email, he called me to address my concern (no email reply). My take away was that the 30 day requirement should be there, but there appears to be some hang-ups within Legal [redacted] that are interested in finding ways to postpone Congressional notifications.

Since the incident back in September 2015 and then again with the Florida incident, it has been extremely difficult to get any written feedback from Matt's Opinions Unit or from [redacted]. Ever since the whole Chokepoint matter became public, it seems like the Legal Division is under some kind of gag order from [redacted]. And, that's why I sent the email below.

I'm still chuckling about how [redacted] engineered the cloak and dagger out of channel "cloak and dagger" mystery pickup of a document that they didn't want to acknowledge in writing on the network. ([redacted] directed an attorney to grab a piece of paper from my desk (no email, no copying, etc.,) and bring it like a piece of road kill back to his unit.

Anyhow, I put the 7 and 30 day provisions into the draft DBMG and legal struck the 30 day reporting requirement and Matt made it an optional one pending further OMB action – which I believe it most definitely not an option. Plus, [redacted] struck the analysis made to simplify the conundrum posed by M-16-03 as my analysis was written for the scope of the audience using the Data Breach Mgmt Guide. Since the scope is limited to a narrower subset of potential incidents, my analysis was easier to use – and made it crystal clear when an incident is a Major Incident and therefore requires Congressional notification under the 7 day FISMA req't.

I'm not sure whether the actions over there are trying to cover-up the Florida incident or are trying to misconstrue what is really pretty straightforward reporting req'ts in FISMA 2014 and OMB M-16-03, but the actions are most definitely helpful with making reporting clear. I think they would prefer to make a muddier set of waters and then not have to report. Dang Chokepoint!

This goes back to the advice I provided [redacted] about covering one's re[redacted]hen you know the law is on your side, but others are trying to keep negative publicity like chokepoint, t[redacted]rida incident, the OCFI incident, and whatever else covered up.

Okay, my self-rant is now complete.

Whether the actions are trying to cover-up the Florida incident ...

One current FDIC OGC employee intimated that [redacted] motivations for issuing the directive in this instance related to Congressional oversight. Specifically, the OGC employee had the following exchange during a transcribed interview:

Q. **Are you aware if there was ever any concern with [redacted], that she either voiced about email communications potentially being responsive to congressional requests or caught up in congressional requests?**

A. **That -- well, yeah, I imagine that was behind it, in part, anyway.**

Q. Okay.

A. That plus the unsettled nature of the issues which were deemed very sensitive at higher levels.[93]

The latter portion of this exchange indicates [redacted] did not want other OGC attorneys to characterize opinions of high ranking FDIC officials on what she deemed sensitive topics – in this case what is deemed a major breach for the purposes of Congressional notification. According to the current FDIC OGC employee [redacted] was the only FDIC official to issue the directive to avoid putting interpretive language in emails and other written documents. However, the totality of the circumstances in this investigation suggest the directive may have been a coordinated strategy to avoid transparency. The record is unclear whether this directive came from higher ranking officials at FDIC.[94] The current OGC witness testified:

Q. And just for clarity sake, what exactly were you told not to talk about in email?

A. I think interpretation of the major incident.

Q. And how was that directive communicated to you?

A. By telephone.

Q. And who communicated that to you?

A. [redacted]

Q. And did you get the impression that was coming just from her, or was that coming from someone else or somewhere else? Just in general.

A. I couldn't say. I don't have a -- [95]

At the full committee hearing on May 12, 2016, committee staff advises Members to probe the Chairman on whether he is aware that Deputy General Counsel [redacted] directed OGC staff not to put legal opinions and analysis in writing – a practice that would render those writings discoverable. This was not the first time [redacted] directed staff not to put things in writing. A current OGC staffer member testified:

---

[93] [redacted] Tr., *supra* note 69, at 22–23.
[94] *Id.*
[95] *Id.* at 53.

Q. I apologize for jumping around a little bit, but as far as matters not being discussed in emails and [redacted] telling you that, is that the first instance of that ever occurring of what businesses that we've been discussing? Are you familiar with any other incidents at the FDIC where someone asked or instructed others not to put something in email?

A. **No, I think she had done it in the past on one or two things, not in this context at all, but just where things were sensitive and perhaps there might be publicity or something, or the thing wasn't cooked yet at a sufficient level of sensitivity that -- but I can't recall particulars.**[96]

Here, the record reflects that this is a pattern of avoiding transparency and free flowing discussion of policies at FDIC. This directive creates inefficiencies for those charged with working on matters [redacted] deems "sensitive." In fact, earlier in this same interview the witness indicated that [redacted] directive hampered OGC staff's ability to have a robust discussion about policy matters with the relevant subject matter experts at FDIC.[97]

Committee staff believe the actions outlined above amount to obstruction of Congressional oversight for which Chairman Gruenberg must answer. Additionally, the FDIC's maneuvering has left the agency in a vulnerable position from a cybersecurity perspective. The Committee will continue to shed light on FDIC's actions to prevent Congressional oversight and the weaknesses in the agency's cybersecurity infrastructure.

## VI. Hearing Witnesses

***Martin J. Gruenberg, Chairman, FDIC***

Martin J. Gruenberg is the 20th Chairman of the FDIC, receiving Senate confirmation on November 15, 2012 for a five-year term. Mr. Gruenberg served as Vice Chairman and Member of the FDIC Board of Directors from August 22, 2005 until his confirmation as Chairman. He served as Acting Chairman from July 9, 2011 to November 15, 2012, and also from November 16, 2005 to June 26, 2006. Mr. Gruenberg holds a J.D. from Case Western Reserve Law School and an A.B. from Princeton University, Woodrow Wilson School of Public and International Affairs.

***Fred Gibson, Acting Inspector General, FDIC***

Fred Gibson is the FDIC's Acting Inspector General. As such, he is responsible for all facets of the OIG's mission, which broadly is to prevent and detect waste, fraud, and abuse

[96] *Id.* at 73.
[97] *Id.* at 55.

affecting the programs and operations of the FDIC and to keep the Chairman of the FDIC and the Congress fully informed. He leads an office of 125 Federal law enforcement officers, auditors and other professionals, with an annual budget of approximately $35 million. Mr. Gibson graduated from the University of Texas at Austin with a BA in History. He holds a Master's degree in Russian Area Studies from Georgetown University, and his JD from the University of Texas School of Law. He is a member of the State Bar of Texas and the Bar of the Court of Appeals of the District of Columbia and is admitted to practice in numerous Federal courts throughout the country.

## VI. Conclusion

The Committee remains concerned about the FDIC's weak cybersecurity posture and its ability to prevent further breaches. Further, the FDIC's repeated unwillingness to be open and transparent with the Committee's investigation raises serious concerns about whether the agency is still attempting to shield information from production to Congress. With these issues in mind, the Committee will continue to investigate the FDIC's cybersecurity, its response to the breaches, and ensure that the Committee receives all of the requested materials necessary to further its inquiry. It is the Committee's responsibility to ensure that agencies covered by FISMA are complying with the statute and thereby protecting federal government information and American's sensitive banking information.