FDIC DATA BREACHES: CAN AMERICANS TRUST THAT THEIR PRIVATE BANKING INFORMATION IS SECURE?

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

May 12, 2016

Serial No. 114–77

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

20–874PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

FRANK D. LUCAS, Oklahoma
F. JAMES SENSENBRENNER, JR., Wisconsin
DANA ROHRABACHER, California
RANDY NEUGEBAUER, Texas
MICHAEL T. MCCAUL, Texas
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
JIM BRIDENSTINE, Oklahoma
RANDY K. WEBER, Texas
JOHN R. MOOLENAAR, Michigan
STEVE KNIGHT, California
BRIAN BABIN, Texas
BRUCE WESTERMAN, Arkansas
BARBARA COMSTOCK, Virginia
GARY PALMER, Alabama
BARRY LOUDERMILK, Georgia
RALPH LEE ABRAHAM, Louisiana
DARIN LAHOOD, Illinois

EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
DONNA F. EDWARDS, Maryland
SUZANNE BONAMICI, Oregon
ERIC SWALWELL, California
ALAN GRAYSON, Florida
AMI BERA, California
ELIZABETH H. ESTY, Connecticut
MARC A. VEASEY, Texas
KATHERINE M. CLARK, Massachusetts
DON S. BEYER, JR., Virginia
ED PERLMUTTER, Colorado
PAUL TONKO, New York
MARK TAKANO, California
BILL FOSTER, Illinois

SUBCOMMITTEE ON OVERSIGHT

HON. BARRY LOUDERMILK, Georgia, *Chair*

F. JAMES SENSENBRENNER, JR., Wisconsin
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
DARIN LAHOOD, Illinois
LAMAR S. SMITH, Texas

DON BEYER, Virginia
ALAN GRAYSON, Florida
ZOE LOFGREN, California
EDDIE BERNICE JOHNSON, Texas

CONTENTS

May 12, 2016

FDIC DATA BREACHES: CAN AMERICANS TRUST THAT THEIR PRIVATE BANKING INFORMATION IS SECURE?

THURSDAY, MAY 12, 2016

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittee met, pursuant to call, at 10:04 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Barry Loudermilk [Chairman of the Subcommittee] presiding.

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

Subcommittee on Oversight

FDIC Data Breaches: Can Americans Trust that Their Private Banking Information Is Secure?

Thursday, May 12, 2016
10:00 a.m.
2318 Rayburn House Office Building

Witnesses

Mr. Lawrence Gross, Jr., Chief Information Officer and Chief Privacy Officer, FDIC

Mr. Fred W. Gibson, Acting Inspector General, FDIC

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HEARING CHARTER

Thursday, May 12, 2016

TO: Members, Subcommittee on Oversight

FROM: Majority Staff, Committee on Science, Space, and Technology

SUBJECT: Subcommittee hearing: *"FDIC Data Breaches: Can Americans Trust that Their Private Banking Information Is Secure?"*

The Subcommittee on Oversight will hold a hearing titled *"FDIC Data Breaches: Can Americans Trust that Their Private Banking Information Is Secure?"* on Thursday, May 12, 2016, at 10:00 a.m. in Room 2318 of the Rayburn House Office Building.

Hearing Purpose:

The purpose of this hearing is to examine recent data breaches at the Federal Deposit Insurance Corporation (FDIC) – one occurring in October 2015, and another in February 2016.[1] Pursuant to the Committee's Federal Information Security Modernization Act of 2014 (FISMA) jurisdiction, the FDIC wrote the Committee about these breaches.[2] The hearing will also examine broader issues surrounding the FDIC's cybersecurity posture.

The FDIC is an independent agency established by Congress, with the mission "to maintain stability and public confidence in the nation's financial system by:

- insuring deposits;
- examining and supervising financial institutions for safety and soundness and consumer protection;
- making large and complex financial institutions resolvable; and
- managing receiverships.[3]

Witness List

- **Mr. Lawrence Gross, Jr.**, *Chief Information Officer and Chief Privacy Officer, FDIC*

---

[1] 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) .
[2] 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).
[3] Federal Deposit Insurance Corporation, 2015-2019 Strategic Plan, Mission, Vision, & Values *available at* https://www.fdic.gov/about/strategic/strategic/mission.html (last visited May 5, 2016).

- **Mr. Fred W. Gibson,** *Acting Inspector General, FDIC*

Staff Contacts

For questions related to the hearing, please contact Caroline Ingram or Drew Colliatie of the Majority Staff at 202-225-6371.

Chairman LOUDERMILK. The Subcommittee on Oversight will come to order.

Without objection, the Chair is authorized to declare a recess of the Subcommittee at any time.

Welcome to today's hearing entitled "FDIC Data Breaches: Can Americans Trust That Their Private Banking Information is Secure?"

I recognize myself for five minutes for an opening statement.

Good morning. We're here today to learn more about cybersecurity breaches at the Federal Deposit Insurance Corporation. As a former information systems technology company owner for over 20 years, I know firsthand the importance of safeguarding sensitive information and private customer data. Regrettably, the American people have good reason to question whether their private banking information is properly secured by the FDIC.

The FDIC is an independent agency established by Congress, with the mission "to maintain stability and public confidence in the nation's financial system." Unfortunately, the FDIC is failing to live up to its mission of maintaining public confidence in the Nation's financial system because the Agency is failing to safeguard private banking information for millions of Americans who rely on FDIC.

During the Committee's current investigation, it has become clear that FDIC has a long history of cybersecurity incidents. According to information obtained by the Committee, in 2011, a foreign government hacked into the workstations of the former FDIC Chairman and other senior officials. It appears that this entity had access to senior officials' workstations for at least one year before the FDIC took remedial action.

More recently, in letters dated February 26, 2016, and March 18, 2016, FDIC notified the Science Committee of two major security incidents. This notification to the Committee was required in accordance with the Federal Information Security Modernization Act of 2014, otherwise known as FISMA, and Office of Management and Budget guidelines that require executive branch departments and agencies to report major security incidents to Congress within seven days.

The security breach reported in FDIC's February 26 letter to the Committee involved an FDIC employee who copied sensitive personally identifiable information, or PII, over 10,000 individuals onto a portable storage device prior to separating from employment at the FDIC. The employee also downloaded suspicious activity reports, bank currency transaction reports, customer data reports and a small subset of personal work and tax files. 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.

Further, according to the information obtained by the Committee, the FDIC did not report the incident to Congress within the seven-day time period as required by FISMA. In fact, FDIC waited for over four months to report the incident to Congress and only did so after being prompted by the FDIC Office of Inspector General.

Just as troubling, FDIC continues to maintain that the employee "accidently" copied sensitive and proprietary information to a portable storage device, despite the fact that the employee initially told the agency that she "would never do such a thing," and even denied ever owning a portable storage device. Ultimately, she retained legal counsel, who engaged in protracted negotiations with the agency for the return of the device.

The second security breach reported to the Committee was on March 18, 2016, involved a disgruntled FDIC employee who obtained sensitive data for over 44,000 individuals prior to separating from employment at the agency. When the employee left the FDIC on February 26, 2016, the employee took the storage device from the premises. Upon learning of the incident three days later, FDIC personnel worked to recover the device. The device was ultimately recovered on March 1, 2016. According to the FDIC, this was just another case of an employee "accidently" leaving the agency with sensitive information.

This week, 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." To date, FDIC has failed to notify any of those individuals that their private information may have been compromised.

According to the FDIC, none of the 160,000 individuals has anything to worry about because all of the FDIC employees who improperly walked out of the agency with sensitive information were required to sign affidavits stating the information was not disseminated. At best, this is a misleading statement because apparently all employees who are separating from the FDIC are generally required to sign an exit document attesting that they have not removed any FDIC materials from the premises. In the recent breaches reported to this Committee, all employees who improperly took the data should have already signed exit documents before ever leaving the agency.

It is Congress's responsibility to shine a light on FDIC's history of cybersecurity breaches. The Committee will continue its oversight of FDIC failures to secure Americans' sensitive information from apparent foreign entities and disgruntled FDIC employees.

I thank the witnesses for being here today and sincerely hope that we are able to get answers from the FDIC here this morning.

[The prepared statement of Chairman Loudermilk follows:]

U.S. House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight

"FDIC Data Breaches: Can Americans Trust that their Private Banking Information is Secure?"

Thursday, 10:00 a.m., May 12, 2016

Statement by Chairman Barry Loudermilk

Good morning. We are here today to learn more about cybersecurity breaches at the Federal Deposit Insurance Corporation (FDIC). As a former software company owner for over 20 years, I know first-hand the importance of safeguarding sensitive information and private customer data. Regrettably, the American people have good reason to question whether their private banking information is properly secured by the FDIC.

The FDIC is an independent agency established by Congress, with the mission "to maintain stability and public confidence in the nation's financial system." Unfortunately, the FDIC is failing to live up to its mission of maintaining public confidence in the nation's financial system because the agency is failing to safeguard private banking information for millions of Americans who rely on FDIC. During the Committee's

current investigation, it has become clear that FDIC has a long history of cybersecurity incidents. According to information obtained by the Committee, in 2011, a foreign government hacked into the workstations of the former FDIC Chairman and other senior officials. It appears that this entity had access to senior officials' workstations for at least one year before the FDIC took remedial action.

More recently, in letters dated February 26, 2016, and March 18, 2016, FDIC notified the Science Committee of two major security incidents. This notification to the Committee was required in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and Office of Management and Budget guidelines that require Executive Branch departments and agencies to report "major" security incidents to Congress within seven days.

The security breach reported in FDIC's February 26th letter to the Committee involved an FDIC employee who 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. The employee also downloaded "Suspicious Activity Reports, Bank Currency Transaction Reports, [Bank Secrecy Act] Customer Data Reports and a small subset of personal work and tax files. 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. Further, according to information obtained by the Committee, the FDIC *did not* report the incident to Congress within the seven day time period as required by FISMA. **In fact, FDIC waited for over four months to report the incident to Congress and only did so after being prompted by the FDIC Office of Inspector General.** Just as troubling, FDIC continues to maintain that the employee "accidently" copied sensitive and proprietary information to a portable storage device despite the fact that the employee initially told the agency that she "would never do such a thing" and even denied ever owning a portable storage device. Ultimately, she retained legal counsel who engaged in

protracted negotiations with the agency for the return of the device.

The second security breach reported to the Committee on March 18, 2016, involved a disgruntled FDIC employee who obtained sensitive data for 44,000 individuals prior to separating from employment at the agency. When the employee left the FDIC on February 26, 2016, the employee took the storage device from the premises. Upon learning of the incident three days later, FDIC personnel worked to recover the device. The device was ultimately recovered on March 1, 2016. According to the FDIC, this was just another case of an employee "accidently" leaving the agency with sensitive information.

This week, 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."

To date, FDIC has failed to notify any of those individuals that their private information may have been compromised. According to the FDIC, none of the 160,000 individuals has anything to worry about because all of the FDIC employees who improperly walked out of the agency with sensitive information were required to sign affidavits stating the information was not disseminated. At best, this is a misleading statement because apparently all employees who are separating from FDIC are generally required to sign an exit document attesting that they have not removed any FDIC materials from the premises. In the recent breaches reported to this Committee, all employees who improperly took the data should have already signed exit documents before ever leaving the agency.

It is Congress' responsibility to shine a light on FDIC's history of cybersecurity breaches. The Committee will continue its oversight of FDIC's failures to secure Americans' sensitive information from apparent foreign entities and disgruntled FDIC employees. I thank the witnesses for being here today and sincerely hope we are able to get answers from the FDIC

here this morning. With that, I recognize the Ranking Member for his opening statement.

Chairman LOUDERMILK. With that, I recognize the Ranking Member for his opening statement.

Mr. BEYER. Thank you, Chairman Loudermilk, and I appreciate your extensive detailing of these breaches.

Defending against cyber threats is a persistent and evolving battle, and the cyber hazards that confront the public and private sectors come in various forms. Hackers can and have wreaked havoc on Hollywood studios, global financial institutions, retail outlets, and public agencies alike, and no one seems immune from the various cyber threats that touch virtually everyone.

Please forgive a certain amount of redundancy in my statement. It's important that we have both parties on record here.

In case of the Federal Deposit Insurance Corporation, they suffered from seven major cyber incidents in the past 7 months, and these breaches include plugging removable media such as a USB drive into an FDIC computer and removing thousands of sensitive financial and other records from the agency as employees walked out the door. We'll be focusing on two of these breaches today, as well as the FDIC's cybersecurity practices.

I'm glad the FDIC has installed new software that allowed them to identify these recent breaches and respond to them. Without that technology, known as data loss prevention tool, these incidents, whether inadvertent or intentional, would have gone unnoticed and unaddressed, and we in Congress would have remained uninformed. And I believe the FDIC Chairman has taken some positive steps in the wake of these breaches, phasing out the use of removable media such as flash drives and CDs that pose increased security risks.

However, I, along with our Chairman, do have questions about why there was such a long delay in notifying Congress about major cyber incidents, particularly the one that occurred last October and was not reported to Congress until February 26, 2016. And in that instance, it took a memo from the FDIC Inspector General's Office to the FDIC CIO reminding the agency that they had an obligation to report the incident to Congress.

I would add that the IG was not the only one suggesting the FDIC notify Congress of the incident. It's my understanding that other FDIC employees had also recommended reporting this to Congress earlier.

In addition, I believe that the new OMB guidance on federal information security and privacy management requirements, as detailed in the OMB memo 16–03 last October, is very clear. If it takes 8 hours or more to recover sensitive data that comprises 10,000 or more records or affects 10,000 or more people, it is considered a major cyber incident.

Under these guidelines, once an agency is aware that a breach meets that criteria, the incident should be considered a major breach and must be reported to Congress within 7 days. This did not happen in either of the two cases this hearing will focus on or the other five that the FDIC just reported to the Committee this week, and I'm still unclear why.

In the October incident, the breach included records from eight banks, more than 40,000 individuals, and 30,000 entities, including the sensitive bank currency transaction reports and Social Security

numbers. Despite the OMB requirement that agencies inform Congress of major incidents within 7 days, FDIC notified Congress nearly 3 months after it had enough data to determine that this was a major breach.

I hope that Mr. Gross, the Chief Information Officer at FDIC, can help explain FDIC's decision to delay notifying Congress in that October incident, and I hope also that you'll be able to help us understand the agency's characterization of the incident, which appears to be at odds with some of the information obtained by the Committee. I know the Inspector General has looked at the October incident and the FDIC's response, so I look forward to Mr. Gibson's testimony as well.

As a business owner, we have a very important responsibility to protect our customer data, which includes Social Security numbers, cell phones, emails, personal addresses, and we do all we can to protect them, especially when an employee leaves, because we know that this has value to the employee in a different role. And we're just a business. We're not the government controlling these really sensitive government records. So this is a very important issue.

And, Mr. Gross, I understand you just arrived at the FDIC in November, and the CIO's office has suffered from a lack of consistent leadership. You're the fourth CIO in the last four years. I hope that you'll be able to bring some stability to this office, and equally important is I hope that you'll help us establish a solid foundation of reliability and openness with Congress and that you'll strive to do that as well.

So thank you both for being with us today, and we look forward to the questioning.

Mr. Chairman, I yield back.

[The prepared statement of Mr. Beyer follows:]

OPENING STATEMENT
Ranking Member Don Beyer (D-VA)
of the Subcommittee on Oversight

House Committee on Science, Space, and Technology
Subcommittee on Oversight
"FDIC Data Breaches:
Can Americans Trust that Their Private Banking Information Is Secure?"
May 12, 2016

Thank you Chairman Loudermilk.

Defending against cyber threats is a persistent and evolving battle. The cyber hazards that confront the public and private sectors come in various forms. Hackers can and have wreaked havoc on Hollywood studios, global financial institutions, retail outlets, and public agencies alike. No one seems to be immune from the various cyber threats that touch virtually everyone.

In the case of the Federal Deposit Insurance Corporation, or FDIC, they have suffered from seven "major" cyber incidents in the past seven months. These breaches involved plugging "removable media," such as an USB drive, into an FDIC computer and removing thousands of sensitive financial and other records from the Agency as employees walked out the door. We will be focusing on two of these breaches today as well as the FDIC's cybersecurity practices.

I am glad that FDIC recently installed new software that allowed them to identify these recent breaches and respond to them. Without that technology, known as a Data Loss Prevention (DLP) tool, these incidents, whether inadvertent or intentional, would have gone unnoticed and unaddressed, and Congress would have remained uninformed. I also believe the FDIC Chairman has taken some positive steps in the wake of these breaches, phasing out the use of removable media, such as flash drives and CDs, for instance, that pose increased security risks.

However, I do have questions about why there was such a long delay in notifying Congress about "major" cyber incidents, particularly the one that occurred last October and was not reported to Congress until February 26, 2016. In that instance, it took a Memo from the FDIC Inspector General's office to the FDIC CIO reminding the Agency that they had an obligation to report the incident to Congress. I would add that the IG was not the only one suggesting that the FDIC notify Congress of the incident. It is my understanding that other FDIC employees had also recommended reporting this incident to Congress months earlier.

In addition, I believe the new OMB guidance on "Federal Information Security and Privacy Management Requirements," as detailed in OMB Memo 16-03 last October, is very clear. If it takes eight hours or more to recover sensitive data that comprises 10,000 or more records or affects 10,000 or more people it is considered a "major" cyber incident. Under these guidelines, once an Agency is aware that a breach meets that criteria, the incident should be considered a "major" breach and must be reported to Congress within seven calendar days.

That did not happen in either of the two cases this hearing will focus on, or the five others that the FDIC just reported to the Committee this week, and I am still unclear why. In the October incident the breach included records from eight banks, more than 40,000 individuals and 30,000 entities, including sensitive Bank Currency Transaction Reports and Social Security Numbers. Despite the OMB requirement that Agencies inform Congress of 'major' incidents within seven days, FDIC notified Congress nearly three months after it had enough data to determine that this was a 'major' breach.

I hope that Mr. Gross, the Chief Information Officer (CIO) at FDIC, who is testifying today can help explain FDIC's decision to delay notifying Congress in that October incident. I also hope he can help us understand the Agency's characterization of this incident, which appears to be at odds with some of the information obtained by the Committee. I know the Inspector General has looked at the October incident and the FDIC's response to it, and I am looking forward to IG Gibson's testimony as well.

Lastly, Mr. Gross, I understand you just arrived at FDIC in November and that the CIO's office has suffered from a lack of consistent leadership for some time. You are now the fourth CIO the FDIC has had in the past four years. I hope that you will be able to bring some stability to that office. But equally important is establishing a solid foundation built on reliability and openness with Congress. I hope that you will strive to do that as well.

Thank you to both our witnesses for being here today and I look forward to your testimony.

I yield back.

Chairman LOUDERMILK. Thank you, Mr. Beyer.

I now recognize the Chairman of the Full Committee, the gentleman from Texas, Mr. Smith.

Chairman SMITH. Thank you, Mr. Chairman. And I appreciate both your comments and the Ranking Member's comments as well.

The recent cybersecurity breaches experienced by the FDIC date back to October 2015 and compromise nearly 160,000 individuals' sensitive information or personally identifiable information. The number of individuals whose information was compromised by the agency's poor cybersecurity posture could be much higher. The breaches reported to Congress represent only those that the agency itself called "major." In reality, the FDIC likely has experienced additional breaches deemed insufficient by the agency to warrant reporting to Congress.

On April 8, 2016, the Committee sent a letter to the FDIC about a February 2016 cyber breach. In that case, more than 44,000 individuals' sensitive information was breached. Less than two weeks later, the Committee sent an additional letter to the FDIC concerning an earlier breach in October 2015, which compromised more than 10,000 individuals' sensitive information. The Committee sent the additional letter to the FDIC because the FDIC withheld reporting the breach to Congress for more than four months. In fact, the FDIC only reported the breach once the Office of Inspector General urged it to do so.

The FDIC's attempts to shield information from Congress did not end with its hesitation to report the significant October breach. The Committee has encountered a pattern of obstruction from the FDIC when responding to Committee requests.

In the FDIC's response to the Committee's letters, the agency initially produced documents extensively redacted for information the agency deemed to be confidential. These redactions included public information, such as the names of senior-level agency employees, whose identities were already known to the Committee.

The FDIC failed to provide statutory authority or a valid privilege for redacting the information. Still, the agency resisted the Committee's request for unredacted documents until faced with the threat of the Committee's use of the compulsory process to obtain the information.

Additionally, the Committee learned that the agency actively obstructed the Committee's ongoing investigation by limiting the scope of documents produced in response to the Committee's requests. The FDIC responded to the Committee's second letter and certified that it produced all responsive documents. However, subsequent discussions with the Office of Inspector General indicated that responsive documents were withheld by the agency.

Upon learning of the agency's active obstruction, the Committee wrote to the Office of Inspector General to request these documents. If not for the Office of Inspector General's openness and transparency with the Committee, we would not have been aware of the Agency's attempts to avoid providing a full and complete response to the Committee.

The FDIC's repeated efforts to conceal information from Congress are inexcusable. They raise significant questions about whether the Agency actively attempts to hide potentially incriminating informa-

tion from Congress. As an agency that has faced repeated security breaches, it should focus its resources on reforming its internal cybersecurity mechanisms instead of engaging in efforts to conceal information from this Committee.

The Committee will continue to investigate the shortfalls in the FDIC's cybersecurity posture and why the Agency continues to withhold certain information from Congress and this Committee. We also will hear what measures the Agency should take to remediate the damage to the tens of thousands of Americans' whose information was compromised.

So, Mr. Chairman, we have a lot to learn this morning and look forward to the testimony of our two witnesses, and I yield back.

[The prepared statement of Chairman Smith follows:]

Statement of Science Committee Chairman Lamar Smith
Oversight Subcommittee Hearing on
FDIC Data Breaches: Can Americans Trust that Their Private Banking Information Is Secure?
10:00 a.m. Thursday, May 12, 2016
FINAL: Caroline Ingram

Thank you, Mr. Chairman.

The recent cybersecurity breaches experienced by the FDIC date back to October 2015 and compromise nearly 160,000 individuals' sensitive information or personally identifiable information.

The number of individuals whose information was compromised by the agency's poor cybersecurity posture could be much higher. The breaches reported to Congress represent only those that the agency has deemed "major."

In reality, the FDIC likely has experienced additional breaches deemed insufficient by the agency to warrant reporting to Congress.

On April 8, 2016, the Committee sent a letter to the FDIC about a February 2016 cyber breach. In that case, more than 44,000 individuals' sensitive information was breached.

Less than two weeks later, the Committee sent an additional letter to the FDIC concerning an earlier breach in October 2015, which compromised more than 10,000 individuals' sensitive information.

The Committee sent the additional letter to the FDIC because the FDIC withheld reporting the breach to Congress for more than four months. In fact, the FDIC only reported the breach once the Office of Inspector General urged it to do so.

The FDIC's attempts to shield information from Congress did not end with its hesitation to report the significant October breach. The Committee has encountered a pattern of obstruction from the FDIC when responding to Committee requests.

In the FDIC's response to the Committee's letters, the agency initially produced documents extensively redacted for information the agency deemed to be "confidential."

These redactions included public information, such as the names of senior-level agency employees, whose identities were already known to the Committee.

The FDIC failed to provide statutory authority or a valid privilege for redacting the information. Still, the agency resisted the Committee's request for unredacted documents until faced with the threat of the Committee's use of the compulsory process to obtain the information.

Additionally, the Committee learned that the agency actively obstructed the Committee's ongoing investigation by limiting the scope of documents produced in response to the Committee's requests.

The FDIC responded to the Committee's second letter and certified that it produced all responsive documents. However, subsequent discussions with the Office of Inspector General indicated that responsive documents were withheld by the agency.

Upon learning of the agency's active obstruction, the Committee wrote to the Office of Inspector General to request these documents.

If not for the Office of Inspector General's openness and transparency with the Committee, we would not have been aware of the agency's attempts to avoid providing a full and complete response to the Committee.

The FDIC's repeated efforts to conceal information from Congress are inexcusable. They raise significant questions about whether the agency actively attempts to hide potentially incriminating information from Congress.

As an agency that has faced repeated security breaches, it should focus its resources on reforming its internal cybersecurity mechanisms instead of engaging in efforts to conceal information from this Committee.

The Committee will continue to investigate the shortfalls in the FDIC's cybersecurity posture and why the agency continues to withhold certain information from Congress and this Committee.

We also will hear what measures the agency should take to remediate the damage to the tens of thousands of Americans' whose information was compromised.

###

Chairman LOUDERMILK. The gentleman yields back.

I now recognize the Ranking Member of the Full Committee for a statement.

Ms. JOHNSON. Thank you very much, Chairman Loudermilk, and thanks to you, our witnesses, for being here today.

All data breaches that expose sensitive personal information should be taken very seriously. In today's digital age, our sensitive personal data is everywhere. When we swipe our credit cards at the grocery store, renew our driver's license at the Department of Motor Vehicles and passports at the Department of State, or visit the emergency room at the local hospital or the bank around the corner, our sensitive, personal, and financial data is processed, stored, and entrusted to those entities to safeguard it and ensure that it is not inadvertently breached or intentionally stolen.

But that has happened seven times in the past 7 months in major cyber breaches at the Federal Deposit Insurance Corporation. None of these breaches were the result of sophisticated hackers, foreign adversaries, or cyber criminals. And those that downloaded this data, including Social Security numbers and suspicious activity reports, did not use high-tech digital tools. They simply plugged in their thumb drives and other removable media to their FDIC workstations in that office and downloaded sensitive, personal, and financial data onto their personal storage devices. These actions jeopardized the data security of thousands of individuals, multiple banks, and potentially criminal investigations.

In virtually every—each of these seven instances the FDIC has said the sensitive data was inadvertently downloaded and that there was no malicious intent. In all of these cases the FDIC was able to recover the data, and the former FDIC employees signed affidavits saying they had not shared the data with others.

However, in at least one case, according to FDIC's own records, a former employee who downloaded such data was evasive about her actions and not cooperative when initially confronted by FDIC staff. Some FDIC employees also suggest that it was highly improbable that this former employee's actions were accidental.

In addition, this former employee is now working for a U.S. subsidiary of a non-U.S. financial services company, which raises additional concerns. I would remind FDIC that in 2013 an Inspector General review of another much more serious cyber accident at the agency resulted in one senior official in the CIO's office leaving the agency and another being demoted.

My understanding is that this response by these former officials to both the Chairman of the FDIC and the IG's office and the Government Accountability Office lacked candor in both of their descriptions of the extent of this penetration and potential consequences to the agency.

I hope IG's office will be able to clarify whether or not all of the recent data breaches were inadvertent, as the FDIC has claimed, when his office completes the two audits they are currently working on regarding FDIC's handling of major cybersecurity incidences in the coming weeks. I also hope that the IG's office can shed some light on the reasons why the office of the Chief Information Officer and the FDIC failed to inform Congress of these major incidences within the 7-day time frame required by the guidance from the Of-

fice of Management and Budget and that issued in the late October 2015.

I believe that FDIC has already taken some positive steps in responding to the recent data breaches, phasing out the use of removable media, for instance. I encourage them to continue to ensure that sensitive data is not intentionally or inadvertently breached, but I would also request that the new CIO, Mr. Lawrence Gross, who is testifying with us today, to keep Congress appropriately and fully informed in a timely manner when major cybersecurity incidences do occur.

I thank you, Mr. Chairman, and my time's expired. I yield back.

[The prepared statement of Ms. Johnson follows:]

OPENING STATEMENT
Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
Subcommittee on Oversight
"FDIC Data Breaches:
Can Americans Trust that Their Private Banking Information Is Secure?"
May 12, 2016

Thank you Chairman Loudermilk, and thank you to our two witnesses for being here today.

All data breaches that expose sensitive personal information should be taken very seriously. In today's digital age our sensitive personal data is everywhere. When we swipe our credit cards at the grocery store, renew our drivers' licenses at the Department of Motor Vehicles and passports at the Department of State, or visit the emergency room at the local hospital or the bank around the corner, our sensitive personal and financial data is processed, stored and entrusted to those entities to safeguard it and ensure it is not inadvertently breached or intentionally stolen.

But that has happened seven times in the past seven months in major cyber breaches at the Federal Deposit Insurance Corporation (FDIC). None of these breaches were the result of sophisticated hackers, foreign adversaries or cyber criminals. And those that downloaded this data, including Social Security Numbers and Suspicious Activity Reports (SARs) did not use high-tech digital tools. They simply plugged in thumb drives and other removable media to their FDIC workstations in the office and downloaded sensitive personal and financial data onto their personal storage devices jeopardized the data security of thousands of individuals, multiple banks and potentially criminal investigations.

In virtually each of these seven instances, the FDIC has said the sensitive data was inadvertently downloaded and that there was no malicious intent. I hope that that is true, but I fear that it is not. In all of these cases the FDIC was able to recover the data, and the former FDIC employees signed affidavits saying they had not shared the data with others.

However, in at least one case, according to the FDIC's own records, a former employee who downloaded such data, was evasive about her actions and not cooperative when initially confronted by FDIC staff. Some FDIC employees also suggest it was highly improbable this former employee's actions were accidental. In addition, this former employee is now working for a U.S. subsidiary of an Indian financial services company, which raises additional concerns.

I would remind FDIC that in 2013 an Inspector General review of another, much more serious, cyber incident at the Agency resulted in one senior official in the CIO's office leaving the Agency and another being demoted. My understanding is that this was not due to FDIC's response to this threat, but the lack of candor by the former officials in the CIO's office in describing the extent of this penetration and the consequences to the Agency to both the Chairman of the FDIC, the IG's office and the Government Accountability Office (GAO).

I hope the IG's office will be able to clarify whether or not all of the recent data breaches were "inadvertent," as FDIC has claimed, or not, when his office completes the two audits they are currently working on regarding FDIC's handling of "major" cybersecurity incidents in the coming weeks. I also hope the IG's office can shed some light on the reasons why the office of the Chief Information Officer (CIO) and the FDIC failed to inform Congress of these major incidents within the seven-day timeframe required by new guidance from the Office of Management and Budget (OMB).

I believe the FDIC has already taken some positive steps in responding to the recent data breaches, phasing out the use of removable media, for instance. I encourage them to continue to ensure that sensitive data is not intentionally or inadvertently breached. But I would also advise the new CIO, Lawrence Gross, testifying before us today, to keep Congress appropriately and fully informed, in a timely manner, when "major" cybersecurity incidents do occur.

Thank you. I yield back.

Chairman LOUDERMILK. I thank the lady. She has yielded back.

Now, let me introduce our witnesses for today. Our first witness is Mr. Fred Gibson, acting Inspector General of the Federal Deposit Insurance Corporation. Mr. Gibson has previously served with the Resolution Trust Corporation Office of Inspector General and as Principal Deputy Inspector General and counsel to the Inspector General.

Mr. Gibson received his bachelor's degree in history from the University of Texas at Austin and his master's degree in Russian Area Studies from Georgetown University. He received his J.D. from the University of Texas Law School.

Our second witness today is Mr. Lawrence Gross?

Chairman LOUDERMILK. Gross. Mr. Lawrence Gross, Jr., Chief Information Officer and Chief Privacy Officer of the Federal Deposit Insurance Corporation. Mr. Gross previously served as the CIO for the U.S. Department of Agriculture, Farm Service Agency and the Deputy CIO at the Department of the Interior.

Mr. Gross received his bachelor's degree in information systems management from the University of Maryland, University College, and he received his CIO certification from the National Defense University.

I now recognize Mr. Gibson for five minutes to present his testimony.

TESTIMONY OF MR. LAWRENCE GROSS, JR.,
CHIEF INFORMATION OFFICER
AND CHIEF PRIVACY OFFICER, FDIC

Mr. GIBSON. Thank you, sir.

Chairman Smith, Ranking Member Johnson, Chairman Loudermilk, Ranking Member Beyer, and Members of the Subcommittee, my name is Fred Gibson, and I'm the acting Inspector General of the Federal Deposit Insurance Corporation. Thank you for the invitation to speak with the Subcommittee today regarding recent cybersecurity incidents at the Federal Deposit Insurance Corporation.

The Federal Government has seen a marked increase in the number of information security incidents affecting the integrity, confidentiality, and availability of government information, systems, and services. The charter for this hearing is to address two specific security interests and concerns that this Committee has regarding the FDIC's cybersecurity posture.

The FDIC's Office of Inspector General carries out two primary functions. The first is to audit and evaluate the FDIC's programs and operations, including controls designed to safeguard the Corporation's data and address and report breaches when they occur. The second function is to investigate suspected criminal activity, including breach incidents where case-specific facts lead us to believe that a crime may have occurred.

With respect to our first role, we are currently conducting two audits pertinent to the Committee's concerns that we anticipate will be completed in the near future. The first examines the FDIC's process for identifying and reporting major security incidents, as required by applicable federal law and related guidance. The second audit addresses the FDIC's controls for mitigating the risk of

an unauthorized release of sensitive information submitted by systemically important financial institutions.

As you are aware, on February 19, 2016, during the planning phase of the first of these audits, we issued a memorandum to the FDIC's Chief Information Officer regarding a specific security incident which we believe warranted Congressional reporting. In the memorandum the OIG concluded that the Corporation was required under the Federal Information Security Modernization Act of 2014 and related guidance issued by the Office of Management and Budget—and that's OMB Memorandum 16–03—to report the security breach as a major incident to the appropriate Congressional committees. Ultimately, the FDIC reported the major incident to this Committee, which led ultimately to our testimony today.

With respect to our criminal investigative function, the FDIC OIG participates as a non-voting member on the FDIC's Data Breach Management Team, or DBMT, for situational awareness purposes. The DBMT, as its name implies, reviews data breach incidents. Where the facts of a particular incident, which we learn through our participation in the DBMT or from other sources, appear to point to a crime having been committed, we open an investigation. If the results of our investigation warrant, we make referrals to the Department of Justice. I can confirm the existence of one criminal investigation arising out of the incidents that formed the basis for today's hearing. However, that case is open. It's in a pre-indictment phase, which limits my ability to discuss it directly.

Nevertheless, I hope to be able to provide you with the information that you need to conduct your oversight activities with regard to these issues, and I look forward to answering the questions that the Committee has. Thank you very much.

[The prepared statement of Mr. Gibson follows:]

Testimony

Before the Committee on Science, Space,
and Technology
Subcommittee on Oversight
U.S. House of Representatives

Cybersecurity Incidents at the Federal Deposit Insurance Corporation

Statement of Fred W. Gibson, Jr.
Acting Inspector General
Federal Deposit Insurance Corporation

May 12, 2016

Statement of Fred W. Gibson, Jr.
Acting Inspector General, Federal Deposit Insurance Corporation
May 12, 2016

House Committee on Science, Space, and Technology
Subcommittee on Oversight

Chairman Loudermilk, Ranking Member Beyer, and Members of the Subcommittee,

Thank you for the invitation to speak with the Subcommittee on Oversight today regarding recent cybersecurity incidents at the Federal Deposit Insurance Corporation (FDIC).

The federal government has seen a marked increase in the number of information security incidents affecting the integrity, confidentiality, and availability of government information, systems, and services. We share the Committee's view that the FDIC needs to ensure that it has proper controls in place to protect the highly sensitive information that it possesses in both its corporate and receivership capacities.

To that end, the FDIC's Office of Inspector General (OIG) carries out two primary functions that have relevance to the subject matter of today's hearing. The first is to audit and evaluate the FDIC's programs and operations, including controls designed to safeguard the Corporation's data and address and report breaches when they occur. The second function is to investigate suspected criminal activity, including breach incidents where the case-specific facts lead us to believe that a crime may have occurred.

With respect to our first role, we are currently conducting two relevant audits that we anticipate will be completed in the near future. The first one is examining the FDIC's process for identifying and reporting major security incidents, as required by applicable federal law and related guidance. The second audit is addressing the FDIC's controls for mitigating the risk of an unauthorized release of sensitive resolution plans submitted by systemically important financial institutions. Because our work is ongoing, I will not be able to discuss conclusions or recommendations that we may offer when these two audits are completed.

However, as you are aware, on February 19, 2016, during the planning phase of the first of our audits, we issued a memorandum to the FDIC's Chief Information Officer regarding a specific security incident warranting Congressional reporting. Information in that memorandum, although marked privileged and for official use only, became public. I can confirm that in the memorandum, the OIG concluded that the Corporation was required under the Federal

Information Security Modernization Act of 2014 and related guidance issued by the Office of Management and Budget (OMB Memorandum M-16-03) to report the security breach as a "major incident" to the appropriate Congressional committees. The FDIC ultimately reported the major incident to the appropriate Congressional committees.

With respect to our criminal investigative function, the FDIC OIG participates as a non-voting member on the FDIC's Data Breach Management Team (DBMT) for awareness purposes. The DBMT, as its name implies, reviews data breach incidents. Where the facts of a particular incident, which we learn of through our participation in the DBMT or from other sources, appear to point to a crime having been committed, we open an investigation. If the results of our investigation warrant, we make referrals to the Department of Justice. Unfortunately, I cannot discuss the details of open criminal investigations related to such breaches at the FDIC with you today.

I would emphasize that because the facts and circumstances of security incidents vary, grounds do not always exist for pursuing a criminal investigation. Where that threshold is not met, the responsibility lies with the FDIC to pursue the civil and administrative remedies that it deems appropriate.

Thank you again for the opportunity to speak with you today and for understanding the limits on what I am able to discuss at this time. I will be happy to answer any questions.

Fred W. Gibson, Jr.
Acting Inspector General

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 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. The OIG conducts investigations of potential fraud and other crimes in insured financial institutions, closed banks, and the FDIC, and audits of the FDIC, including its supervision, resolution, complex financial institution, and information security programs.

Mr. Gibson is an attorney by profession, specializing in banking, securities, and corporate law. He practiced for 12 years with regional and national law firms in Texas and Washington, DC, before joining the Resolution Trust Corporation (RTC) Office of Inspector General as a Senior Attorney in 1992. He has served with the RTC and FDIC Offices of Inspector General since that time. Prior to becoming Principal Deputy Inspector General, he served as Counsel to the Inspector General. In that capacity, he provided independent legal services to the Inspector General and the managers and staff of the OIG. He concurrently served as a Special Assistant United States Attorney (Criminal Division) for the Southern District of Florida.

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.

Chairman LOUDERMILK. I now recognize Mr. Gross for his opening statement.

TESTIMONY OF MR. FRED W. GIBSON,
ACTING INSPECTOR GENERAL, FDIC

Mr. GROSS. Chairman Loudermilk, Ranking Member Beyer, and Members of the Subcommittee, thank you for the opportunity to appear before you today.

At the FDIC, protecting sensitive information is critical to our mission of maintaining stability and public confidence in the Nation's financial system, and we are continually enhancing our information security program.

My name is Lawrence Gross, and I am FDIC's Chief Information Officer and Chief Privacy Officer. I assumed my duties at the FDIC in November of 2015, and I have more than 39 years of combined military and federal sector experience in the information technology, law enforcement, cybersecurity, and critical infrastructure fields. My testimony today will focus on our program to identify, analyze, report, and remediate incidents based on the risk of harm they pose.

The FDIC has a strong information security program to identify events that could signal a data security incident, including mandatory annual training for all employees and contractors to ensure that they will be alert to inadequate protection of sensitive information and know when and how to notify our Computer Security Incident Response Team.

We also have automated monitoring tools, including the data loss prevention tool, which scans for sensitive information in outgoing emails, uploads to Web sites, and any data downloaded to portable media from FDIC systems. Our goal is to assess and continually improve our situational awareness so that we can reduce and ultimately eliminate the risk of harm to individuals and entities.

The FDIC has a security incident response and escalation plan to ensure the systemic gathering and analyzing of facts relevant to an event to determine the risk of harm and the taking of appropriate action. We then take steps to mitigate the risk of harm and complete the appropriate reporting and notifications based on the risk of harm.

With the passage of FISMA in late 2014 and the subsequent issuance in October of OMB guidance on what constitutes a major incident, we have further refined our incident reporting regime. Notably, the new law and OMB's guidance have been applied to incidents over the past 6 months where FDIC employees departed employment and were identified by our monitoring tools as having downloaded personally identifiable information or other FDIC-sensitive information on portable media not long before their departure.

It was my initial judgment, based on several factors, that these incidents did not rise to the level of major incident as defined in the OMB guidance. In each case, the employee had legitimate access to the sensitive data in question while at the FDIC. Further, our analysis indicated the downloading of the PII was inadvertent. The FDIC recovered the data from the former employees, and there was no evidence that the former employee had disseminated the

data. And all the former employees assigned affidavits affirming they had not disseminated the data beyond themselves.

Lastly, in each case, the circumstances surrounding the employees' departure were non-adversarial. Under these circumstances, I judged the risk of harm to be very low, meaning that the reporting of these incidents would fall under the annual FISMA-notification-to-Congress requirement.

However, our Office of Inspector General reviewed one of these incidents and came to a different conclusion. Although our interpretations are different, we nevertheless gave such notification to Congress within seven days, and I further directed my staff to go back through all incidents that had occurred since issuance of the OMB guidance, regardless if they were closed, to identify any incidents that had characteristics we thought would meet the OIG's interpretation of major incident. FDIC has now reported those as well to Congress.

Finally, let me touch on changes we have made or are making to lower the risk of future incidents. We've implemented a plan to eliminate the ability of employees and contractors to download to portable media. We're implementing digital rights management software that prevents copying of information. Further, I've directed my staff to begin immediately a top-to-bottom review of IT policies and procedures with the focus on those for departing employees to ensure that everyone understands FDIC policy regarding downloading of data. Also, I will be engaging an independent third party to conduct an end-to-end assessment of all the key areas of the IT security and privacy programs.

The global interconnected landscape continues to evolve, and the threats continue to develop. The FDIC takes very seriously cybersecurity incident management and transparency as it relates to our reporting requirements and remains committed to maintaining a robust IT security program that ensures a real-time current view of our situational awareness.

Thank you again for the opportunity to testify, and I would be happy to answer any of your questions.

[The prepared statement of Mr. Gross follows:]

STATEMENT OF

LAWRENCE GROSS
CHIEF INFORMATION OFFICER AND CHIEF PRIVACY OFFICER
FEDERAL DEPOSIT INSURANCE CORPORATION

on

INFORMATION SECURITY

before the

SUBCOMMITTEE ON OVERSIGHT
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

May 12, 2016
2318 Rayburn House Office Building

Chairman Loudermilk, Ranking Member Beyer, and members of the Subcommittee, thank you for the opportunity to appear before you today to discuss the important issue of cybersecurity, including our efforts to identify and address information technology (IT) security incidents. At the FDIC we are keenly aware that protecting sensitive information is critical to our mission of maintaining stability and public confidence in the nation's financial system and we are continually enhancing our information security program.

My name is Lawrence Gross and I am the FDIC's Chief Information Officer and Chief Privacy Officer. I assumed my duties at the FDIC in November 2015. As the Chief Information Officer and Chief Privacy Officer, I am responsible for providing executive leadership and oversight of the FDIC Information Technology, Privacy, Information Management, and Information Security programs. I have more than 39 years of combined military and federal sector experience in the information technology, law enforcement, cybersecurity and critical infrastructure fields. My testimony today will focus on our program to *identify, analyze, report, and remediate* incidents based on the risk of harm they pose to individuals or entities we supervise.

Identification

The FDIC has a strong information security program to *identify* events that could signal a data security incident. For example, we have mandatory annual training for all employees and contractors to ensure that they will be alert to inadequate protection of sensitive information, and know when and how to notify our Computer Security Incident Response Team (CSIRT). Employees have self-reported when they have had access to sensitive information beyond what

was needed to perform their job. This is one example of a low risk incident. We also have automated monitoring tools and analysts responsible for reviewing reports from these tools on a daily basis. One example of automated monitoring is our Data Loss Prevention tool, which scans for sensitive information in outgoing emails, uploads to web sites, and any data downloaded to portable media from FDIC systems. Another tool monitors which web sites employees and contractors attempt to visit in order to prevent access to sites that may pose a risk to the agency. Our goal in the FDIC information security program is to assess and continually improve our situational awareness and shed light on events so that we can reduce and ultimately eliminate the risk of harm to individuals and entities.

Analysis

The FDIC has a security incident response and escalation plan to ensure the systematic gathering and *analyzing* of facts relevant to an event to determine the risk of harm to individuals or entities and the taking of appropriate action. When there is an elevated risk of harm, an interdisciplinary team meets to review the facts surrounding the incident and provide the CIO a recommended course of action. This team, the Data Breach Management Team (DBMT), has been in place for several years. I chair the DBMT meetings, membership on which includes representatives from the Office of the Inspector General (OIG), our Chief Risk Officer's office, the Chief Information Security Officer, our Legal Division, the division or office where the incident took place, and several others. This inter-disciplinary team works through a standardized procedure to gather facts, analyze the facts to determine the risk of harm to individuals and entities, and recommend a course of action for each incident.

Security incidents can range from situations where monitoring tools detect that a retiring employee copied sensitive information to portable media immediately prior to departing employment, to the theft of sensitive bank examination papers from an examiner's automobile, to the discovery of an external, adversarial entity attempting to breach our network defenses. In each of these cases, the incident would be reported to the Computer Security Incident Response Team (CSIRT) and, if the risk of harm is elevated, the DBMT is convened to analyze the incident. The analysis may consist of reviewing the amount and type of records potentially exposed, the circumstances surrounding the incident, and the actors involved. The DBMT asks questions and directs the gathering of additional information to gauge the risk of harm to individuals and entities in order to form a recommendation for an appropriate course of action.

Reporting

After we have gathered and analyzed the relevant incident facts, we take steps to mitigate the risk of harm, and complete the appropriate *reporting* and notifications based on the risk of harm. For example, we have had instances in the past where a thief has broken into an FDIC bank examiner's car and stolen a locked case of work papers containing bank borrower or depositor Personally Identifiable Information (PII). In those instances, the DBMT has quickly recommended notification of the individuals and the financial institutions, and the offering of credit monitoring. Another example has been when an examiner's laptop is stolen. One of the features of our information security program is that our examiner's laptop hard drives are encrypted. Since the probability of a petty thief breaking our encryption algorithm and using any PII on the laptop to cause harm is low, notifications of individuals are not typically warranted. However, all of these incidents are reported to the Department of Homeland Security's US-

CERT, to the Office of Management and Budget (OMB) in our annual Federal Information Security Management Act (FISMA) submission, and to Congress annually.

With the passage of FISMA in December 2014, and the subsequent issuance on October 30, 2015 of guidance by OMB concerning what constitutes a "major incident", we have further refined our incident reporting regime. Notably, the new law and OMB's guidance on "major incident" have been applied to incidents over the past six months where FDIC employees departed employment and were identified by our monitoring tools as having downloaded PII or other FDIC sensitive information to portable media not long before departure. It was my initial judgment that these incidents did not rise to the level of "major incident" as defined in the OMB guidance. I based my decision on several factors. In each case, the employee had legitimate access to the sensitive data in question while at the FDIC; our analysis indicated the downloading of the PII was inadvertent; the FDIC recovered the data from the former employees; there was no evidence that the former employee had disseminated the data; and, the former employee signed an affidavit stating they had not disseminated the data. Lastly, in each case, the circumstances surrounding the employee's departure from FDIC employment were non-adversarial. The totality of the circumstances led to my judgment that, in each case, the former employee inadvertently downloaded the FDIC-related information while he or she was attempting to download personal files in preparation for departure. Under these circumstances, I judged the risk of harm to be very low, meaning that the reporting of these incidents would fall under the annual FISMA notification to Congress requirement.

However, our OIG reviewed one of these incidents and came to a different conclusion. The OIG, in a memorandum dated February 19, 2016, recommended that the incident they

reviewed be reported to Congress under the category of "major incident". Although our interpretations differed, we nevertheless gave such notification to Congress within seven days, on February 26, 2016. In addition, I directed my staff to go back through all incidents that had occurred since October 30, 2015, on which we had already made determinations, to identify any incidents that had characteristics we thought would meet the OIG's interpretation of "major incident" and the FDIC has now reported those as well to Congress.

Remediation

Recognizing the potential risk associated with the use of portable media, we have taken additional *remedial* steps to further lower the risk of sensitive information being exposed through this channel. Several changes we are making as part of a sixty day review to lower the risks of future incidents are highlighted below.

- We have implemented a plan to eliminate the ability of employees or contractors to download to portable media (such as DVDs, CDs and flash drives). We have already implemented technology to remove the ability of the majority of employees to download any data from FDIC systems to portable media. For those members of our workforce whose business processes continue to require that they use this technology, we are actively working to identify and implement alternative means to securely exchange data with entities such as our state banking department counterparts by the end of 2016. In addition, as of Friday, May 13, software will force encryption of portable media in those instances when business processes require continued use.

- We are implementing Digital Rights Management (DRM) software to better protect our most sensitive information. The purpose of DRM is to prevent unauthorized redistribution of digital information. DRM can prevent or limit copying, and can limit the time period in which the content can be accessed, among other features. DRM technology can provide an efficient preemptive approach to the challenges of data exfiltration when compared to reactive technologies that identify issues after the fact.
- In addition to technological changes I have highlighted, I have directed my staff to begin immediately a top to bottom review of all current FDIC IT policies and procedures with a focus on revising policies and procedures for departing employees, and ensuring IT security policies associated with IT security incident management are current and incorporate recent changes in OMB guidance. This policy review and revision initiative will ensure that current and departing employees understand the policy and are aware of the requirements in downloading any data, personal or business, and we will provide them with the assistance to do so where appropriate.
- Finally, I will be engaging an independent third party to conduct an end-to-end assessment of the FDIC IT Security and Privacy Programs. The program review will encompass all key areas of the FDIC's IT security program including: network security, software security, host security, data protection, identity and access management, threat and vulnerability management, asset management, security monitoring and compliance, third party management, privacy, business continuity management, incident management, data infrastructure (i.e., events, alerts, and logs), policies and standards, awareness and training, program metrics and reporting, and governance and organization. The resulting analysis will identify any potential gaps in the FDIC's security and privacy programs and

outline a mitigation plan with measurable remediation steps required to address gaps, vulnerabilities and risks identified.

Conclusion

The global interconnected landscape continues to evolve and the threat and threat actors continue to develop tools and techniques to thwart our IT defenses. The FDIC is committed to meeting this evolving challenge by refining our operational policies and procedures on an ongoing basis to meet and mitigate the evolving threats. The FDIC takes very seriously cyber security, incident management, and transparency as it relates to our reporting requirements and remains committed to maintaining a robust IT security program that ensures a real time current view of our situational awareness. This real time view is essential to our ability to protect against and mitigate cyber related incidents proactively. That concludes my opening remarks. Thank you again for the opportunity to testify today. I would be happy to answer your questions.

Lawrence Gross

Chief Information Officer & Chief Privacy Officer

BIO

On November, 2, 2015, the FDIC Board of Directors approved the appointment of Lawrence Gross, Jr. to the position of FDIC Chief Information Officer (CIO). Mr. Gross in his role as CIO reports directly to the Chairman and provides leadership to the Division of Information Technology and the Information Security and Privacy functions and operations. Further, Mr. Gross serves as the chief advisor to the Chairman, Board members, and senior executive managers on all strategic issues relating to information technology (IT), including governance, investments, program management, strategic planning, privacy and security. Mr. Gross has more than 39 years of combined military and federal sector experience in the information technology, law enforcement, cybersecurity, and critical infrastructure fields.

Prior to his appointment at the FDIC, Mr. Gross served as the CIO for the U.S. Department of Agriculture, Farm Service Agency (FSA). In addition to his leadership role at the Farm Services Agency (FSA), Mr. Gross served for five years as the Deputy CIO at the Department of the Interior where he was responsible for the management and oversight of Interior's .5 billion dollar IT portfolio and operating budget, as well as providing day-to-day executive leadership and strategic direction to IT federal and contractor staff.

Mr. Gross holds a Bachelor of Science degree in Information Systems Management from the University of Maryland, University College, and he holds a CIO Certification from the National Defense University. Mr. Gross is a member of several professional information technology-related organizations, and is the recipient of several prestigious military and civilian awards including the Presidential Award for leading the Federal Financial Management Line of Business Initiative, the Department of Energy's, Secretary's Award for Leadership in Electronic Government, the Department of Justice, Attorney General's Award, and the Federal 100 Award which recognizes government and industry leaders who have played pivotal roles in the federal government IT community—individuals who have gone above and beyond their daily responsibilities and have made a difference in the way technology has transformed their agency or accelerated their agency's mission.

Chairman LOUDERMILK. I thank the witnesses for their testimony.

And just before we begin our questions, for the witnesses and the Members of the Committee, it is the Chair's intention to be somewhat lenient with the clock because it is important that we do get these questions answered and as many rounds of questioning as we need. The Chair is ready to extend this hearing as long as we need to make sure that all the questions are adequately answered.

And also to our witnesses, we ask that you be very truthful, as well as comprehensive, but also we have had incidents of filibustering answers. And again, the Chair will maintain the Subcommittee going as long as we need to, to make sure. So we ask that you be as accurate and as brief with your answer.

I now recognize myself for five minutes for questioning.

Mr. Gross, this Committee wrote the FDIC requesting documents and communications referring or relating to the security breaches we discussed here today. Are you aware of those letters?

Mr. GROSS. I am.

Chairman LOUDERMILK. The FDIC has certified that all responsive documents pursuant to this Committee's request had been produced. Is that your understanding as of today?

Mr. GROSS. I believe the office has been responsive to your inquiries, sir, yes.

Chairman LOUDERMILK. Mr. Gross, did anyone in your office, to your knowledge, voice any concern regarding the manner, scope, or have any other concerns about the FDIC's response to this Committee's request?

Mr. GROSS. No one in my office had any concern with being responsive——

Chairman LOUDERMILK. No one expressed any concerns about the documents you were providing?

Mr. GROSS. No one in my office expressed any concerns, sir.

Chairman LOUDERMILK. What about other offices, anyone in the FDIC express concerns about the comprehensiveness of the investigation or the documents you're providing?

Mr. GROSS. I'm not aware of anyone expressing any concerns.

Chairman LOUDERMILK. No one in the FDIC. Mr. Gross, are you aware of any internal FDIC documents responsive to the Committee's request that were not produced to this Committee?

Mr. GROSS. I'm not aware of any that have not been provided, sir.

Chairman LOUDERMILK. Mr. Gibson, to your knowledge, were all responsive documents produced to this Committee?

Mr. GIBSON. Sir, was that direction—was that question——

Chairman LOUDERMILK. I'm sorry. Yes, I'm sorry. Mr. Gibson, that was directed to you. I was looking at Mr. Gross. Sorry.

Mr. Gibson, to your knowledge, were all responsive documents produced to this Committee?

Mr. GIBSON. Sir, we haven't reviewed the FDIC's production of documents to the Committee. We received a request from the Committee for FDIC documents that were in our possession, and we provided the documents that we collected in the context of our audit.

Chairman LOUDERMILK. Okay. So, Mr. Gross, just to summarize and make sure we understand, to your knowledge, you provided all the documents that were responsive to the Committee's request?

Mr. GROSS. To my knowledge, sir, we were responsive to the request. If there's a request for additional information, I'll stand ready to provide that.

Chairman LOUDERMILK. Okay. Thank you.

Mr. Gross, what I have here 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 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.

Chairman LOUDERMILK. So let me make sure I understand what your statement here is today, that everything that you provided is also covered in the IG's? There's no more information in what the IG provided to us than what is covered in this stack of documents here?

Mr. GROSS. I can——

Chairman LOUDERMILK. Is that what you're telling me?

Mr. GROSS. I cannot make that as an affirmative statement, sir. I had a brief opportunity to review the IG's material yesterday——

Chairman LOUDERMILK. Okay.

Mr. GROSS. —so I cannot say that it's a one-to-one correlation.

Chairman LOUDERMILK. Well, you were saying it was duplicative——

Mr. GROSS. I said——

Chairman LOUDERMILK. —but——

Mr. GROSS. —quite a bit of the material that was in there was duplicative. There was multiple copies, for example, of the Data Breach Management Guide. There are multiple copies of that guide provided in their response to you.

Chairman LOUDERMILK. Okay. There are many emails that were provided to us by the IG that were not included in your documents. Those are not duplicative.

Mr. GROSS. I cannot speak to that without looking at the exact emails, but what we have in the incident response summary might be—well, I would think it's an encapsulation of what may be contained in emails that were transmitted between different entities that participated on the DBMT.

Chairman LOUDERMILK. Okay. Okay. But you did say that you had reviewed the materials——

Mr. GROSS. I did——

Chairman LOUDERMILK. —provided——

Mr. GROSS. I did a cursory review.

Chairman LOUDERMILK. A cursory review——

Mr. GROSS. Yes.

Chairman LOUDERMILK. —but you have not looked at them. When were these—Mr. Gibson, when were these documents provided?

Mr. GIBSON. Sir, I believe they were provided at ten o'clock yesterday morning.

Chairman LOUDERMILK. Okay. Has Mr. Gross received copies of these documents?

Mr. GIBSON. Yes, sir. We provided a copy of our—I don't know if Mr. Gross personally has. We provided a copy of our production to the Congress to the FDIC so they would be aware of what we did.

Chairman LOUDERMILK. And when was that provided?

Mr. GIBSON. At the same time we provided it to the Committee.

Chairman LOUDERMILK. So ten o'clock yesterday morning?

Mr. GIBSON. Yes, sir, about ten o'clock.

Chairman LOUDERMILK. Okay. Allow me to clear my desk for a moment here. Okay.

So, Mr. Gross, you still stand by that—your previous testimony that you did provide this Committee all the documents that we requested?

Mr. GROSS. That wasn't my statement, sir. I said I believe we were responsive to your request. If there is additional documents that you think are necessary or required, I stand ready to deliver that.

Chairman LOUDERMILK. Okay. So you're acknowledging that there may not be some documents that we requested that the FDIC——

Mr. GROSS. I believe——

Chairman LOUDERMILK. —failed to provide us?

Mr. GROSS. I believe our response to you was responsive. If there's other material or additional material that you deem that's warranted, I stand ready to provide that.

Chairman LOUDERMILK. So you will provide every document that we request?

Mr. GROSS. If there's a request for additional information, we stand ready to provide that.

Chairman LOUDERMILK. Okay. Well, we requested the information the IG has actually provided as well. We're just asking for it to be comprehensive and all-inclusive.

And so who's responsible for providing the documents in response to the Committee's request?

Mr. GROSS. When your letter came in and when the letter came in for the information, that's sent to each of the offices that may have relevant information. Each of those offices then provide that information. It's a—there's a coordination effort that's done by our Office of Legal Affairs, and then it's put together as a comprehensive package for submission.

Chairman LOUDERMILK. Were any directions—to your knowledge, were any directions given to withhold or not provide certain documents to this Committee?

Mr. GROSS. No, sir.

Chairman 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.

Chairman LOUDERMILK. I do have other questions, but I have run over the clock. I was a little more lenient with myself than I intended to be. I do have more questions. The Chair's intention is to do a second round of questioning.

And so at this time I recognize the Ranking Member, Mr. Beyer.

Mr. BEYER. Thank you, Mr. Chairman. And thanks again to the witnesses.

Mr. Gross, are you aware—to follow up on Chairman Loudermilk's questions—of any documents requested by the Committee that you have not submitted yet?

Mr. GROSS. No, sir, I'm not aware of any.

Mr. BEYER. So at this point if anything's missing, you'd be happy to provide it?

Mr. GROSS. Yes, sir, I will.

Mr. BEYER. And I hope—are you willing to have your—you and your staff carefully go through Mr. Gibson's documents to make sure that anything he provided that you didn't that you affirm its value or its legitimacy? I'm trying to get—you pointed out that one reason the stack of documents are so different was there's many duplications, things provided again and again in Mr. Gibson's documents. I think what the Chairman is concerned about is, is there anything Mr. Gibson provided that you didn't?

Mr. GROSS. I understand. I can go through the material and review that and provide you any additional information that you may need or want. I haven't had a full opportunity to review the material, as he's indicated. I received it at 10 o'clock yesterday.

Mr. BEYER. So we're 24 hours away. So—but you're willing to do the reconciliation?

Mr. GROSS. Yes, sir, I am.

Mr. BEYER. Great. Great.

The employee in the October breach reportedly left the FDIC on good terms. She was seeking new employment at the time, and she currently works for a foreign financial firm. Furthermore, she initially denied that she had downloaded the information. She resisted turning over the device to the FDIC, and we understand she was having personal problems at home, she was going through a divorce, she was living in a hotel room. All these factors highlight increased security risks, not mitigating factors, especially as outlined by the FBI and the U.S. counterintelligence community, as this brochure "The Insider Threat" details.

Were these facts known by the Data Breach Management Team when the incident was being analyzed for risk of harm?

Mr. GROSS. All the circumstances surrounding the incident was known by the Data Breach Management Team. I'd like to even go back further and state that we—personally, I make a concerted ef-

fort to be very transparent in all the activities that we have within the security realm. This incident, when it occurred, it actually occurred prior to the promulgation of the OMB guidance, so it was in fact reported in 2015 in our annual FISMA report.

It was my encouragement to the staff that we knew that the policy had come out as we were reviewing this incident, and I asked that they apply the standard of the policy to the incident. So we fully understood the circumstances surrounding it, yes, and we applied the standard to the incident to ensure that we were being responsive. But it had already been reported as part of our FISMA submission.

Mr. BEYER. Okay. So let me break these up. On the one hand, you're arguing that the 7-day didn't apply because the OMB guidance didn't come out until January, but the greater concern is whether it was low risk, moderate risk, or high risk. And we know that this person had gone to work for a foreign bank, had initially denied downloading, refused to turn over the drive, and was going through a lot of personal problems. Don't all those elevate the sense of risk that your—the breach team would consider and that you would consider as CIO?

Mr. GROSS. I considered all the factors associated with the incident. We weighed all the factors. But I would say even if an individual leaves their employment with the Federal Government, we leave with not only potentially material that on removable media, we leave with corporate knowledge. And we still trust that the individuals leaving federal service is going to protect not only that digital media that they may take, but the corporate information they may take in their head. So that had to be weighed as to what risk of harm did the information that this individual inadvertently download pose.

And yes, we considered what type of employment she may have been seeking outside the organization and other factors, and we deemed that the incident was in fact low.

Mr. BEYER. In your testimony on page 4 you talk about that your initial judgment in all these incidents didn't rise to the level of the major incident as defined by OMB guidelines. But the OMB guidelines talked about 8 hours to restore the data, more than 10,000 records affected. Weren't more than 10,000 records affected in virtually every one of these cases?

Mr. GROSS. Yes, sir, they were. Several of these incidents just barely met the threshold that we just retroactively reported.

I think the larger issue is not only does the policy say that there's time-specific parameters for reporting, but it also says in the very end of the document that it's left to the discretion of the agency to determine if in fact the agency has sufficient information to determine if the incident rises to the level of a major. That was considered as part of the review of the policy and the incident.

Mr. BEYER. I don't want to harp on this too much, but you'll forgive us if there's a certain amount of skepticism of seven different people downloading information just as they're leaving that affects more than 10,000 records, and none of them seem to rise to the level of major incident.

Mr. GROSS. Well, it's—in—from my perspective it's not a question of whether or not we're going to report. The agency has no relief

in reporting. The issue that we were looking at was what was the time frame that the reporting was required. If there's a 7-day notification or a 30-day notification or if it's included in the annual FISMA report, you'll find that the FDIC is very responsive. And if you review our FISMA report, you will find that we report all incidents. There is no incidents not reported.

Mr. BEYER. One more question right on this part of it. You said that in each of these cases the downloading was inadvertent.

Mr. GROSS. Yes, sir.

Mr. BEYER. Once again, I have a hard time understanding how you could inadvertently download 10,000 customer records or bank records.

Mr. GROSS. The individuals involved in these incidents were not computer proficient. We have policies in place that will allow the FDIC IT staff to assist you when you're departing the organization to copy down things that you may have collected over your long tenure with the agency, specifically, photographs or your personal resume.

The fact that they were not computer proficient, if you go in and you don't copy the material and do it as a targeted copying of that information, you could in fact inadvertently copy the entire hard drive. So if you insert and you do the copy and not being proficient in the technology, you may take more data than what you intended.

Mr. BEYER. I would certainly hope as you—you talked about the many steps going forward. I think a major step going forward would be to make sure that all that personal information isn't on their computers and that there isn't a way to download an entire—I just—I'm glad you're making progress because all of this sort of boggles the mind that somebody could go in and download an entire disc or all the information that the FDIC has on record about companies and individuals.

Mr. GROSS. Well, sir, I arrived at FDIC in November. As you see from my resume, I've been in federal service to this country for 39—actually, it'll be 40 years in July. I'm an IT professional, and there were several areas that I focused on immediately upon arriving, one of which was removable mobile media, as well as the elimination of the need for being able to do that as a common business practice.

Mr. BEYER. Great. Great. Well, thank you very much, Mr. Gross. Mr. Chairman, I yield back.

Chairman LOUDERMILK. Thank you, Mr. Beyer.

Being 30 years in the IT world, I find it very disheartening that you give someone who is not computer proficient access to such sensitive data. Maybe someone will address that.

I now recognize Mr. Posey, the gentleman from Florida.

Mr. POSEY. Thank you very much, Mr. Chairman.

Mr. Gross, you and I are just viewing this incident from completely different perspectives. You make it sound like this is a very friendly termination from an employee, she accidentally took personal information about 160,000 or more citizens, and then gladly gave it back, just for one example. And the staff kind of tells me it didn't really work out that way all the time, that there was some defiance there, some refusal.

You mentioned there was no evidence that she kept any of the information. Actually, there's no evidence that she didn't keep the information. One went to work for a foreign financial institution that could benefit greatly from mining that kind of data, we know that.

And, you know, I'm amused by the term—the whole issue. We call it a data breach. You know, where I'm from we'd call it a theft. If you take something that's not yours, that's called a theft. We don't call it a data breach back home. Maybe just because we're talking about electronic records, we're no longer going to call it a theft, we're going to call it a data breach. But the fact is tens of thousands of American citizens are compromised because of this.

And my question for you, Mr. Gibson, in your testimony you stated that "If the threshold for criminal investigation is not met, the responsibility lies with the FDIC to pursue the civil and administrative remedies." Could you expound upon what these remedies could potentially be? Surely there will be clear punitive measures for the perpetrators of such a breach. Are there—any of these former employees currently on administrative leave, getting a full paycheck, receiving a pension like the IRS people were? There needs to be consequences for these actions.

Mr. GIBSON. Sir, as a former employee, they're not on payroll, and I do not believe that any of these individuals have retired or are receiving pensions, but I don't know for sure. I believe that they all left for other employment opportunities in other places.

With respect to the FDIC's remedies, both administratively and civilly, the FDIC can pursue the return of information. The FDIC could take actions to enjoin an individual from using, disseminating, taking any action with respect to that information. The FDIC could undertake administrative actions within the FDIC in order to tighten up its security protocols or other situations. There's a number of things they can do in the absence of criminal activity, and that's what I'm really referring to.

Mr. POSEY. Okay. But just on a practical basis, you know, somebody walks into a retail store without the owner's permission and steals 160,000 items, the store owner comes back and figures out somebody stole this, went to them, they say, oh, okay, well, I'll give you back these particular items is all I'm going to admit that I accidentally took from your store. That doesn't eliminate the fact that there was a theft from the store just because they gave back at least some of the items that they illegally took. Do you see any similarity to the example I'm drawing and what happened here?

Mr. GIBSON. Well, sir, I understand the example that you're using, and I would agree in that particular situation. I mean, the fact that somebody robs a bank and gives the money back doesn't mean that they didn't rob the bank. That's absolutely right.

For us to pursue a criminal case, however, one of the things that we're going to have to be able to establish in connection with our case is specific intent on that person's part. If the material was removed inadvertently, which is the FDIC's conclusion with respect to that, we have a bar right up front to being able to pursue a criminal case in the face of that determination. I'm not saying that we can't, but we're going to need some facts that get us over that and allow us to be able to pursue that sort of a case.

Mr. POSEY. Have you exhausted the questioning of the people involved? Have they voluntarily come forth? Do you need to depose them? Are you in a position to—you could depose them and ask the kind of questions you'd like to see answers to and I'd like to see answers to?

Mr. GIBSON. Sir, we—when we conduct a criminal investigation, we do so when we have probable cause to believe that there's been a crime that's been committed. Prior to that time, we conduct something called an inquiry. And the methods that we use in conducting that are somewhat less intrusive than the methods that we would use to conduct an investigation.

When information comes to us where we are able to open an investigation, we do. And in one of these cases, we have. If additional information were to come forward to us that would enable us to open a case, we certainly would be asking those questions. We try and develop it as best we can, and that's the way in which we're pursuing it.

Mr. POSEY. Thank you for your frank answers. I see my time is up. I thank you, Mr. Chairman.

Chairman LOUDERMILK. The Chair recognizes the gentlewoman from California, Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman.

I understand from your testimony that in some instances the Data Breach Management Team recommends that individuals or financial institutions be notified of the breach of personally identifiable information and then credit monitoring can be offered and that that has not been done in this case or in the five other major breaches. Mr. Gross, can you explain why that hasn't happened, what was the thinking here, and are individuals adequately protected without this credit monitoring opportunity?

Mr. GROSS. We evaluated each of the cases and determined because there was low risk of harm that there were no individuals that were affected or impacted adversely as a result of the downloading of the information. So as a result of the lack of impact to the individuals, it was deemed that credit monitoring was not warranted.

We have in other cases where the information has been taken and we know it was a known adversary or someone with adverse intent where they may break in an employee's car and steal records, we know that that individual had ill intent by breaking in the car. That information, regardless of the number of records that may have been exposed, in those cases we would have offered credit monitoring, as we've done in the past.

Ms. LOFGREN. But we don't have digital rights management on these files at this point, do we?

Mr. GROSS. We don't have digital rights management deployed across the FDIC at this moment. It is one of the 60-day response activities that I've laid out for the IG.

Ms. LOFGREN. So we don't know for sure whether this information that was taken was not in fact further copied because there was no DRM to prevent it?

Mr. GROSS. Well, we have the signed affidavit from the employees a——

Ms. LOFGREN. Right.

Mr. GROSS. —and each of these employees——

Ms. LOFGREN. Well, technologically, we have no assurance of that?

Mr. GROSS. Technologically, no, ma'am.

Ms. LOFGREN. I'm interested in the DRM response that you're recommending. I'm interested in what is the timeline. And also, did you—what process was used to determine what DRM response would be—did you do an RFP, was it sole-source, did you do market research? How did you select which DRM solution and what's the timeline for implementation?

Mr. GROSS. I'm working very aggressively to implement it. This is something that we're just beginning to pursue. I don't have the specifics for you at this moment. I could come back to you with a more detailed plan.

Ms. LOFGREN. Oh, so you haven't actually begun that?

Mr. GROSS. We have begun the process of identifying the technology from the standpoint that we think that the right tool for protecting the data is DRM. What solution set and the timeline for implementing it, we have not identified that as yet. We've looked at two technologies. We didn't put that in the report. We didn't want to advocate for any specific vendor, but we are looking at two right now as the potential tools that we would employ.

Ms. LOFGREN. Well, I'm interested in whether you might conduct a pilot with different offerings. I mean, this is an important decision for the agency.

Mr. GROSS. Absolutely, it is. And one of the things that we have to look at is we want to make sure that we don't break the business, that means we have to do this focused on the data that is the most sensitive and work our way out. So yes, we are not going to do this as a wholesale change across the organization because it's—not only do we have to evaluate if there's any internal impact, we have to evaluate is this going to create an impact with the businesses that we have to work with in the conduct of the mission.

Ms. LOFGREN. Just a final note, I was interested in your comment that employees that are leaving are permitted to download their personal information on their computer. And my suggestion would be there shouldn't be any personal information on the government computer.

You know, people do dumb things. I—we once had a young person who downloaded BearShare who migrated all kinds of sensitive information unwittingly. You should create technological barriers to doing that, and if someone manages to subvert that, they should lose their personal information.

I'm just sort of interested in what technological methods have you deployed to prevent the migration of potentially harmful data from outside of your system.

Mr. GROSS. Ma'am, I've arrived at FDIC in November, and I can assure you that there are several things that we've already begun to implement, but there are several other things that we'll be looking at implement going forward.

One of the messages to my staff is that security is not something that we bolt on after the fact. It's something that we include as part of the process from implementation moving toward. So I've identified a number of things in the 60-day plan, but I can assure

you that those are immediate actions that we need to take because of these incidents that we've seen, but there are others that I'm fully looking to employ based on the years of experience knowing that it's about protecting the data and that we do have individuals that may do things mistakenly and we have to manage that. But we also have to manage for external adversarial threats as well. So I can assure you this is just the beginning of some of the things that will be implementing.

Ms. LOFGREN. I see my time is expired, Mr. Chair.

Chairman LOUDERMILK. The Chair recognizes the gentleman from Illinois, Mr. LaHood.

Mr. LAHOOD. Thank you, Mr. Chairman. And I want to thank the witnesses for being here today.

I would just say at the outset, it is troubling to me to hear your response to Mr. Beyer's questions, almost a dismissive nature of these breaches and kind of the nonchalant answers that you've given, particularly with the backdrop of cyber attacks on this country.

We hear every week in this Committee about the cybersecurity and how, at the highest levels of our government and in the private sector, computers are compromised every single day. And you look at—whether it's Chinese entities or Russian mob or domestic enterprises in the United States, I don't think anybody has any confidence that we have this under control. And it leads to a lot of uncertainty about how we tackle this issue.

And so when I hear about an agency, the FDIC, and the information that you control, it's concerning to me that you don't highlight this as an important breach and further investigation to find out what's at stake here. That's really concerning to me to hear that today.

Let me ask some specific questions here. Mr. Gross, in your opening statement you state that the downloading of the personal identifiable information in all the breaches FDIC reported to Congress was "inadvertent" and "non-adversarial." Is that accurate?

Mr. GROSS. That's correct, sir.

Mr. LAHOOD. I want to direct your attention to Exhibit one, which is a document sent by the FDIC legal department to one of the former FDIC employees who left the agency with unauthorized materials on a portable storage device. According to this document, which is dated December 2, 2015, when asked about her actions, she said "she would never do such a thing." And that it would be against FDIC policy and that she knows the policy. When asked if she owns an external hard drive, she said she did not know what an external hard drive is. And she stated that "in any event, she does not own such a device."

Now, Mr. Gross, do you stand by your statement that this person is non-adversarial?

Mr. GROSS. Sir, if I could, one, I'd like to draw the scale because in your opening comment you mentioned the difference between the current incidents and if we had a third-party bad actor in our system. And I don't want to be dismissive. Any loss of information, regardless of how that information is lost, is significant. It's important, and we need to pay attention to it.

I think what we have to do is to draw to scale, though, the different incidents that we have. If there was a third-party actor in my system today, the way the policy is currently constructed, unless that third-party has taken an amount of records, it may not meet the criteria of a major, but I can assure you, if there was a bad actor in our system today, it would be reported as a major, especially if I know that they're adversarial in nature and they intend to do harm to the organization or the agency. I could care less if they were reading the menu for the FDIC. If it's a bad actor and they're in our system today, it is reported, and it falls into the major category.

These incidents where we had employees that left had multiple years of faithful service to the FDIC. These are different circumstances.

Mr. LAHOOD. I understand that, Mr. Gross. My specific question that I asked you, I—the exhibit that's up there, I mean, do you stand by the statement that this person is non-adversarial?

Mr. GROSS. I do. And let me give some context. When the employee departs the FDIC, they sign a document indicating that they have not taken any information with them. When we go back to that employee and we have proof, because of our DLP capabilities, that in fact they have downloaded information, at that instance that conversation is an employee who now realized I've made a mistake. And as a result of that, that relationship has to be managed from the standpoint of a trusted employee who now realizes that they inadvertently took information, and now they're caught misrepresenting the truth.

So I do stand by that from the standpoint is I believe that the employee inadvertently took the material and now they find themselves in an awkward situation where their closing statement doesn't match the actual facts.

Mr. LAHOOD. Yes. Well, I understand your statement, what you're saying there. I mean, this is not a foolproof system. It clearly is not. And the nature of the world we live in now with cyber attacks and foreign entities and what's out there, that's what's, I guess, concerning about the protocol that you went through here.

Let me follow up. So was she telling the truth when she said "she would never do such a thing"?

Mr. GROSS. I believe she, on the surface, was telling the truth, but I don't think she really understood that she had taken—one, I think she realized she took her personal data. I don't believe she realized she took FDIC-specific data. And in each of these cases, these are all referred to the IG's office. Every one of these cases we had asked the IG if they were going to investigate the case. The response we received is that there was no criminal activity; therefore, it did not warrant any further action on their part.

Mr. LAHOOD. Mr. Gibson, let me ask you. Do you agree with Mr. Gross that this person was non-adversarial?

Mr. GIBSON. So I really need to take a look at this set of facts. Offhand, I'd say that there are different interpretations of these facts. Non-adversarial, I mean, it seems to me that you could interpret these facts to suggest that she is adversarial. You could certainly interpret these facts to suggest that she's being less than candid or truthful.

Mr. LAHOOD. And so you don't necessarily agree with that statement and they have a different opinion, is that fair to say?

Mr. GIBSON. Sir, I don't agree with that statement, and I may have a different opinion.

Mr. LAHOOD. I see my time is expired. Let me just ask another question here.

I'm going to refer to Exhibit number two. Mr. Gross, this is an email dated April 28, 2016, to you from the acting Chief Information Security Officer at the FDIC. The message says, "We were notified of the $10,000 record count of these incidences on April 27, so the seven-day reporting requirement will be on May 4, 2016." Mr. Gross, what incidents is the acting Chief Information Security Officer referring to?

Mr. GROSS. I'm not really sure from just looking at this document, but I believe what he's talking about are one of the incidents that we retroactively went back and looked at.

Mr. LAHOOD. And you understood the seven-day reporting period, correct?

Mr. GROSS. Actually, this may have been an incident that was reviewed by the DBMT and already deemed as closed. Without actually looking closer at the document and getting the other information, I'm not sure of that. But we went back retroactively, and some of the incidents that we reported, they had already been reviewed by the DBMT and it had been deemed a breach but a low-risk breach.

Mr. LAHOOD. Did you report the incident to Congress by May 4, as required by the law?

Mr. GROSS. I don't know if this incident was reported by May 4. I believe it was reported in the recent report where we provided five different incidents to the Congress.

Mr. LAHOOD. Yes. I mean, in looking at what the—information I have, it was not reported within the seven days, and actually, it appears on May 9 it was reported, so it was outside of that window. Do you disagree with that?

Mr. GROSS. I don't agree or disagree without looking at—but I believe this was included in the report for all of the incidents. My question would be is was this incident previously closed by the DBMT and deemed as a low-risk? So therefore, the seven-day clock would have actually started long before we completed the record count. It would have been back when the incident may have been initially reviewed.

Mr. LAHOOD. Well, when I look at this document, it looks like this—I mean, clearly, in that quote that I sent to you, you're notified of the incidents on April 27 and told that it has to be done by May 4. It appears that it's outside that window. I guess it just as a follow-up, Mr. Gibson, should incidents such as this that we're discussing today be reported to Congress within a timely manner?

Mr. GIBSON. Sir, I think that when the waterfall requirements of 16–03 are triggered, I think that there's an obligation to report in 7 days from the time that the agency has a reasonable basis to believe that a major incident has occurred. That's what the law says.

Mr. LAHOOD. It appears from this document in Exhibit two that that was the case and it wasn't done within the seven-day period.

Mr. GIBSON. So it could. I haven't—I'm not familiar with the incidents that that's referring to and, you know, to answer that conclusively, I want to review that. But, you know, it certainly could indicate that, yes.

Mr. LAHOOD. Thank you. I went over my time.

Chairman LOUDERMILK. The Chair recognizes himself for questions.

Mr. Gross, the Florida incident, is that one of the incidents that Mr. LaHood was referencing that you believed was inadvertent?

Mr. GROSS. I believe all of the incidents that have been reported were identified where the individual inadvertently downloaded the material.

Chairman LOUDERMILK. And how many incidents has that been?

Mr. GROSS. I believe we've reported seven.

Chairman LOUDERMILK. Seven and they were all accidental?

Mr. GROSS. Out of the seven, we had—I believe it was five individuals that were retiring, and I believe the other individuals were term employees and they were coming to the end of their term.

Chairman LOUDERMILK. Were all seven of these those that you described as not very computer literate or——

Mr. GROSS. Yes, sir, I would say that these individuals downloaded the information in an attempt to take their personal information prior to departure.

Chairman LOUDERMILK. But they had access to sensitive information even though they were not "computer literate"?

Mr. GROSS. Well, the information they had legitimate access to was required for them to perform their day-to-day duties. Their duties continued up until the day they left employment with the FDIC.

Chairman LOUDERMILK. So it's common practice to allow personnel to download information from the FDIC official server?

Mr. GROSS. Prior to my arrival, we did utilize mobile media, and individuals could download information to those devices. We've since put into place capability to prevent the downloading of information to mobile devices.

Chairman LOUDERMILK. So is it accepted practice to allow personal use of the government computers? If they were taking personal information, then obviously they're allowed to use them for personal——

Mr. GROSS. Policy does allow de minimis use of the personal computer, yes, sir.

Chairman LOUDERMILK. Does—do any of the employees in the FDIC, yourself or any others, use personal email to conduct official business?

Mr. GROSS. No, sir, not that I'm aware of.

Chairman LOUDERMILK. None at all. Regarding the Florida incident, the Data Breach Management Team, did they give you a recommendation on whether this was a breach?

Mr. GROSS. The Data Breach Management Team is a group of representatives across the organization. The Inspector General sits on that group. It's not a voting body. It's a consensus body, and they do provide a recommendation. And I believe from the Florida incident that they did recommend that it was a breach, but we did also indicate it was a low-level breach.

Chairman LOUDERMILK. Okay. Well, let me read from you an email which you were just provided a copy. This was from the former CIO Christopher Farrow to you, and—regarding the Florida incident and just item number seven, "Only you can declare this incident a breach. You have not done so. The DBMT has only recommended that this is a breach. We're waiting on you to declare this a breach."

I'm bringing attention to this email that was provided to us by the IG, and it was sent to you on November 30, 2015. And in the subject line it refers to the October 2015 Florida incident that you informed this Committee of. And the subject line says "action required, Florida incident."

As we've discussed here, the body of the email concerns the handling of the incident completely within the scope of the documents requested by this Committee. The IG provided us this document, but you did not, sir. Now, how is not including this email with the documents you provided us being responsive to the Committee's request?

Mr. GROSS. Sir, I believe every effort was made to be responsive to your request. If there's needs for additional information, as I said, I stand ready to do so. I believe this document right here is summarized in our response in the incident management.

Chairman LOUDERMILK. But, sir, did the Committee's request ask for summaries or did it ask for the documents? I believe our request was for all documents, not summaries of documents, but documents.

Mr. GROSS. Sir, I believe our response to the Committee's request was comprehensive. We made an active effort to provide a comprehensive response to this Committee.

Chairman LOUDERMILK. But evidence that you have in front of you is that it was not comprehensive.

Mr. GROSS. I don't know for sure if this was included in the overall submission to the Committee, sir.

Chairman LOUDERMILK. It was not, but the IG did provide this to us.

Are you aware, sir, that actively—by not providing this, you are actively obstructing this Committee's investigation?

Mr. GROSS. Sir, I believe our submission to you was comprehensive. Every effort was made for it to be comprehensive.

Chairman LOUDERMILK. But, sir, it wasn't comprehensive if we're receiving documents from the Inspector General that are clearly relating to these incidents that we are investigating but you did not provide them.

Mr. GROSS. Well, I didn't provide all the documents that you received, sir. These documents came from a variety of different offices within the Corporation.

Chairman LOUDERMILK. But, sir, you are the addressee on the email with this document, so clearly you did have this document. And it would have been your responsibility to provide this in response to our request for all documents.

Mr. GROSS. I believe that this would have been included in the incident response because this document speaks to what's summarized in the incident report.

Chairman LOUDERMILK. But again, sir, the Committee did not ask for summaries; we asked for documents. And are you aware that obstructing Congress is a violation of federal law?

Mr. GROSS. I'm fully aware of that, sir. I'm a prior law enforcement officer.

Chairman LOUDERMILK. Okay.

Mr. GROSS. As I said, we made every effort to be responsive. I believe what we provided was a representation of the production. We made every effort to be quite exhaustive in our response to this Committee. As I said, I—we stand ready to provide any additional information that you deem warranted.

Chairman LOUDERMILK. Well, I thank you for that, but I would prefer that we get these initially and not have to go back and get—let me read directly from the correspondence this Committee sent to you. It says, "All documents and communications referring or relating to the security incident." All documents and communications. We didn't ask for summaries; we asked for all documents and communications, which you failed to provide.

Let me ask you another question. We'll shift our direction of questioning here. Sir, if a bank were to have the incidents happened to them, an employee walks out with a USB drive containing 10,000 pieces of PII of their customers, and they followed the same procedure that you followed by not reporting it to the FDIC, what would the FDIC's actions be to that bank?

Mr. GROSS. I can't speak to that, sir. That's speculative. I——

Chairman LOUDERMILK. I would like to get the answer to that because I don't think it would be following the same procedures that you're holding yourself accountable to.

Maybe, Mr. Gibson, do you know what action would be taken to a bank?

Mr. GIBSON. Sir, I think that question would need to be answered by the supervisors.

Chairman LOUDERMILK. Okay.

Mr. GIBSON. I'm afraid I can't.

Chairman LOUDERMILK. I did pose that to—a question to a banker yesterday, and I will get a formal response of what he believes would have—the action that would have been taken.

Mr. Gross, it appears the FDIC has a history of cyber security breaches that goes beyond what has been made public to date. I personally have a problem after 30 years of being in the information systems business that seven repeated incidents are all inadvertent.

But let's move on to other incidents. Is it true that an "advanced persistent threat" was able to penetrate the FDIC computer systems in August 2011?

Mr. GROSS. I believe that's correct, sir.

Chairman LOUDERMILK. Okay. Is it true that FDIC employees' computers were accessed by a foreign entity without their knowledge?

Mr. GROSS. I believe you're speaking from an Inspector General report, sir, and that, I think, would be best discussed by the Inspector General. That document has sensitive information in it.

Chairman LOUDERMILK. Mr. Gibson, do you have any information that you can share with us?

Mr. GIBSON. If you want to ask me a question, let's see.

Chairman LOUDERMILK. Is it——

Mr. GIBSON. I don't see why not.

Chairman LOUDERMILK. Is it true that FDIC employees' computers were accessed by a foreign entity without their knowledge——

Mr. GIBSON. Sir——

Chairman LOUDERMILK. —dating back to August 2011?

Mr. GIBSON. That is my understanding, yes, sir.

Chairman LOUDERMILK. Okay. Thank you. Mr. Gross, is it true that the Chairman of the FDIC's own computer was accessed by this foreign entity?

Mr. GROSS. Sir, I have reviewed that document. I believe what you're stating is included in the report, but I just became familiar with that document yesterday. I think Mr. Gibson would be best positioned to respond.

Chairman LOUDERMILK. Mr. Gibson, can you respond? Is it true that the Chairman of the FDIC's own computer was accessed by this foreign entity?

Mr. GIBSON. Sir, that's my understanding.

Chairman LOUDERMILK. That's your understanding. And again, this is in an IG report?

Mr. GIBSON. Sir, there are actually—well, there is—I believe the document that you've got is an IG report.

Chairman LOUDERMILK. Okay.

Mr. GIBSON. That document was produced to address the FDIC's handling of the incident internally. It's not a technical report.

Chairman LOUDERMILK. Okay.

Mr. GIBSON. The technical reports would have been prepared by an FDIC contractor that was brought in to study the specific situation. The question is a technical one. Our report really doesn't get to that. It gets more to the issue of reporting of the incident and the FDIC's handling of the incident than it does the technical aspects.

Chairman LOUDERMILK. Okay.

Mr. GIBSON. But in so far as—you know, yes, the answer to the questions that you're asking is yes, but I don't know the technical details——

Chairman LOUDERMILK. Okay.

Mr. GIBSON. —behind some of that.

Chairman LOUDERMILK. Mr. Gross, is it true that the foreign entity was China?

Mr. GROSS. Sir, I don't know that to be correct. I can only tell you what I've read in the report. The details surrounding the report, it happened prior to my arrival.

Chairman LOUDERMILK. I understand.

Mr. GROSS. I can assure you that if that was to happen today under my watch, I'm a prior military person and I believe in the command structure, so if there's an incident that occurs in my organization, one, it's my boat. I'm responsible for making sure it's reported and addressed.

Chairman LOUDERMILK. Well, I understand that and I appreciate your response there. But in the report, does it identify anywhere—

Mr. Gibson, in the report does it identify that the foreign entity was indeed China?

Mr. GIBSON. No, sir, it is not.

Chairman LOUDERMILK. It does not.

Mr. GIBSON. We are not authorized to make a specific attribution to any particular actor.

Chairman LOUDERMILK. Okay. Thank you.

Mr. Gross, regarding this particular incident where supposedly China had access to FDIC computer systems for over a year, which I think would be a very significant issue to maybe have more information on than what we're sharing here today, according to the materials provided to the Committee, the FDIC chose to intentionally violate its own policies and procedures and did not notify CSIRT, the central national authority responsible for tracking, analyzing, and coordinating responses to computer security incidents that attack U.S. Government systems. Is this true?

Mr. GROSS. Sir, as I said, I've reviewed that report, and it's actually great to kind of draw that to scale. When you look at the APT that you're mentioning here versus an incident where we have trusted employees that left the organization, you can see why we drew the fact that the risk of harm to individuals were low. In this instance, if there was an APT in our environment, we would be taking active steps to address it.

But I would have to defer to Mr. Gibson on the specifics that might be contained in the report as to who might have been penetrated or the extent of the penetration into the environment.

Chairman LOUDERMILK. Mr. Gibson, can you provide any more enlightenment in whether they followed proper procedures by notifying a foreign entity?

Mr. GIBSON. They did not.

Chairman LOUDERMILK. They did not. Thank you.

Mr. Gross, it's my understanding that one of the steps taken by the FDIC to prevent further breaches was to shut off the use of USB drives on the computers at the FDIC. What percentage of the FDIC employees roughly still have access to their USB drives?

Mr. GROSS. I believe we've reduced that number down to probably less than 50 percent. We still have a significant number. Our goal is zero. As I said, I've come from other federal agencies, so my goal is to reduce that down to zero. However, we have to work through different business processes that still require the use of that, and what I mean by that is our examiners have a need to exchange information with their 50 different counterparts that they work with in the field. So I can't immediately drive down to zero, but I can assure you and the Committee my goal is to get to zero on use of mobile media within the organization.

Chairman LOUDERMILK. So with the 50 percent that you have disabled, were those the employees that have access to the type of the information that was breached, or are those the 50 percent still remaining to be blocked?

Mr. GROSS. The 50 percent that we had are primarily examiners that work out in the field and other components of the organization that still have an express business requirement for that. The goal, as I said, is zero. In our examiner area, we are actually rolling out technology right now which we call our ETS system.

Chairman LOUDERMILK. Right.

Mr. GROSS. As we roll that out, we will begin to be able to have larger numbers of those groups no longer have a need for the use of mobile media. So we're going to do this over time in specific business areas to be able to get to that zero threshold.

Chairman LOUDERMILK. So if you had these 50 percent—let me ask it this way. If the 50 percent you have blocked now was done six months ago, would it have prevented these incidents?

Mr. GROSS. I can't say that for certain, sir, because these individuals were in various different parts of the organization. And even, as I said, it was an inadvertent download of the data.

Chairman LOUDERMILK. What have you done to prevent it from happening other than the USB drives?

Mr. GROSS. Actually, what we've done to prevent it is we've, one, eliminated the use of mobile media across the organization only to those individuals that require it in order to complete their business processes. In order for those individuals to be able to use the removable media, it requires the approval of their division director.

Chairman LOUDERMILK. Okay.

Mr. GROSS. The—in addition to that, what we're also putting in place is encryption—is that any device that's placed into the machines, once that device is placed in the machine, it will automatically be encrypted. So those mobile devices that we do have in the environment would in fact have encryption, which would enhance their—the security on those devices if they're lost.

Chairman LOUDERMILK. But it would not have prevented these actions from taking place?

Mr. GROSS. I don't believe it would have.

Chairman LOUDERMILK. Mr. Gross, it's interesting that some of these breaches were retroactively reported to Congress. It's clear that the OMB guidance and FISMA state anything over 10,000 instances of PII is to be reported to Congress. We have systems in place to trigger awareness at various government levels. If I go to the bank and withdraw $10,000 of my own money, that is immediately going to be reported, but certain employees at FDIC can download 10,000 individual PIIs and it's not flagged. Is that a double standard?

Mr. GROSS. Well, actually, sir, it is flagged. I think we have a best practice in the fact that we're using DLP to identify those instances. Prior to DLP, we would have been unaware that the employees were downloading that information.

Chairman LOUDERMILK. But there was 10,000 that were breached that were disclosed or taken but you did not report those within the seven-day window.

Mr. GROSS. Sir, it's—we don't have relief in reporting. I want to be—I want to go back to that in that it's not a question of whether or not if it's going to be reported. All incidents within the FDIC are reported. The question is, is it reported within 7 days, 30 days, or is it reported in an annual FISMA report.

So I want to make sure that it's understood is that there's no question about our transparency in reporting. It was in which time frame. And we wanted to draw to scale—we wanted to focus on, is this major? Is this an APT? Is this someone in our system? If we report on incidents that we have deemed as non-major, then we're

reporting on everything. And then when we have an APT or a significant event, the risk you run is that these incidents are then lost in the noise. And I would hate to classify any incident as just noise. But we want to make sure that we're focusing our energies and our time around those incidents that pose significant risk of harm to individuals or the organization.

Chairman LOUDERMILK. Okay. I have been very lenient with my time, and I will do the same to my good friend from Virginia, Mr. Beyer, who is now recognized.

Mr. BEYER. Thank you, Mr. Chairman.

Mr. Gibson, in your testimony you said that the memorandum that you had prepared on February 19 this year to the Chief Information Officer was marked privileged and for official use only, and it was later leaked, which is how come we know about it. Why wasn't it public in the first place? And what's the argument for keeping something like that from the public?

Mr. GIBSON. Sir, it's not our responsibility to report; it's the FDIC's responsibility. We prepared that document in the middle of an audit, actually planning for an audit. We had not completed our work at that point in time. At the time that our work is completed, we would have made some public disclosure of it. There are other points at which public disclosure might have occurred, depending upon the FDIC's response to that memorandum. When they responded by determining that they would disclose the incident, then there was no need for us to make it public ourselves.

Mr. BEYER. In the seven incidents we're talking about that the FDIC and the CIO have all determined were inadvertent, does the decision—or the determination of inadvertency make it more difficult for you to pursue criminal charges?

Mr. GIBSON. Well, sir, it could. It's a fact that you'd have to consider as you evaluate the case. When we have a statement from the government that says that something's inadvertent then you have to establish that there's specific intent to violate the law. Now, if I was a defense lawyer, that's probably the first document that I would wave around. That doesn't mean we can't, but it does mean that it can increase the bar; it can increase the level of difficulty that we have.

Mr. BEYER. Great. Thank you.

Mr. Gross, one of the things I want to be clear about, too, because you've mentioned a number of times your distinguished 39-year career in the military and the federal office, and we thank you for that and thank you for your service. But I just want to also clarify that the hearing is not about your remarkable career but rather about what's going on with the FDIC right now.

In your attempt to remove the mobile media devices down to 50 percent and rolling out ETS, how then will examiners share data if the mobile devices are gone?

Mr. GROSS. We're identifying technology solutions that will allow them to exchange information. As I said, since arriving, I've been looking at the business practices that we have within the organization trying to identify other solutions that will allow us to conduct our business without exposing the data.

Mr. BEYER. Which will include not being able to email the data back and forth?

Mr. GROSS. That's correct. We currently monitor email, and we have the ability to manage or prevent email exchange. But in the case of mobile media, it—just as it says, the ability for a person to move it from point A to point B is quite easy.

Mr. BEYER. I want to clarify one thing you said earlier, and I'm confused. So in the OMB guidance, on the one hand, if it affects more than 10,000 records, it triggers the 7-day response. You also said that it's your classification, major, minor, intermediate, that determines 7-day, 30-day, annual disclosure. Are those in conflict? Do you really have the discretion as CIO to determine what's major and what's not major and therefore what—or, to be specific—because something released 11,000 records and you still determine it not major?

Mr. GROSS. Actually, sir, in the incidents that we've reported, we have several in there that just barely meets the bar. I believe there's a couple that are 13,000 records. The policy is a—it provides some guidance to the agency to consider in making a determination of, one, the significance of an event. So you can have an incident and it's not considered a major in that the surrounding issues around the incident doesn't warrant the 7-day reporting.

Mr. BEYER. Even though it has more than 10,000 records?

Mr. GROSS. In——

Mr. BEYER. Is the 10,000 records threshold not de facto sufficient——

Mr. GROSS. I——

Mr. BEYER. —for the 7-day reporting?

Mr. GROSS. I believe it draws a bright line, and that bright line is that—is what we're following now. But I believe what happens is it creates an environment where you're reporting everything and—as a major, and then you run the risk that if you have a significant event, it would be—it may be overlooked. But the policy clearly says it leaves to the discretion of the agency if there's significant enough information to warrant reporting as a major.

Mr. BEYER. Okay.

Mr. GROSS. But I want to be clear, there's not a question of if the incident is reported. It is reported. The question is in what time frame is it reported.

Mr. BEYER. Well, and I—I'd ask you, please, to listen carefully to this, too, because if anything over 10,000 constitutes so many reports that it's noise, we have a much bigger problem. We should have very few incidents ever that have more than 10,000 records.

Mr. GROSS. I would hope, sir, that we get to zero. My goal by removing the mobile media where we have seen these incidents occur is that we have better management of control of our data. But as you—if you read through the incidents, our employees are fully aware of their requirements of reporting, so we're focused today on removable media.

But on a day-to-day basis, you may have employees that may inadvertently have access to information that was unintended. That could be they saw—they looked at a file share that was online where the permissions may not have been removed. Is that a major? Well, there may be 10,000 records in that file share that they inadvertently saw during that period of time, but was it dur-

ing the normal course of their business so it's not reported as a major, but we still report it as an incident in our FISMA report.

Mr. BEYER. You say that in determining whether major, minor incident, that you used their signed statements, their affidavits to determine that the information has not been disseminated. That seemed to put an awful lot of trust into one signed statement. Are there any other steps you did, tests to see whether any of these records had leaked out, had been sold, had been contacted? For example, the FEC assaults its FEC reports with fake names so they can determine whether somebody else has pulled it off the internet and used it inappropriately.

Mr. GROSS. We do have a forensic review that we conduct on the device once it's returned. One, we can identify if the device that was returned is in fact the device that was used to make the copy. We can also examine the files that are on the document to ensure that we've in fact recovered all of the information that was exfiltrated onto the device originally. But in addition to that, we can determine the last time the files were opened or accessed.

There are limitations to what we can do with the forensics, but it gives us a better perspective as to what happened to the data from the time it was downloaded to the device to the time the device was returned to the organization.

Mr. BEYER. Is there any way to determine whether that data was downloaded into another computer or sent to someone else?

Mr. GROSS. We have limited capabilities in our forensic that we can determine some things but we have to rely on the fact that the employee's assertion that it has not been disseminated beyond themselves is important.

Mr. BEYER. Yes. Once again, I fear that that's going to be too low a bar. But let me move on.

Is the—on the personal information, Ms. Lofgren from California pointed out how probably important it is that the personal information be in fact de minimis, and if it's de minimis, there should be very little that needs to be taken off.

I served four years in State Department, and at the end didn't need to download a single thing. I did have to go delete emails to my wife as to what time I was coming home for dinner but nothing else beyond that. And it's sort of hard to imagine that I would need it—after serving four years that there—or even 30 years that there's much that you'd need to take off the computer.

Mr. GROSS. By implementing the procedures that we have in place for preventing the downloading of the material to mobile media, what that does is put us in a position that if an employee in fact does want to download information, we in fact have to intervene and do that with them on their behalf. So I believe we'll be able to meet that bar that she's indicated where we should be.

We want to make sure that if the employee does have information that they may have created through de minimis use of the device, creating of a resume or other material, that in fact they can take that. But by eliminating their ability to download it, I believe we're in a better position to manage that.

Mr. BEYER. Okay. One last question. On the October breach you made the determination that it couldn't be classified as a major incident, but you have the DBMT, the Data Breach Management

Team. And they all have a—are they simply advisory or do they have a vote in determining what's a major and what's a minor event?

Mr. GROSS. It's not a voting body. All of the representatives on the group—as I said, the Inspector General sits on the group. We have a representative from each of the program areas where the incident may have occurred. They provide a recommendation based on the information to the CIO of whether or not it's a breach, but they also make other recommendations of things that should be considered as part of the review process.

Mr. BEYER. Do you remember whether the—what recommendation the DBMT made in response to the October incident?

Mr. GROSS. I'm not sure the—when you say October incident, is that the Florida incident? That's the one we refer to as——

Mr. BEYER. The original one, yes.

Mr. GROSS. —the Florida incident. I believe it was recommended that it was a breach but it was low risk.

Mr. BEYER. Okay. Have you been in the position yet of having to make a determination that differed from what the DBMT recommended?

Mr. GROSS. No, I don't believe so. And I want to be clear is that the DBMT doesn't meet once. So on the surface it may appear that these incidents may have lingered on or we were nonresponsive. In fact, the DBMT meets on a number of different times during an incident as additional information becomes available, but I don't know of any incidents where I have been in—I've had a difference of opinion of what came out of the DBMT.

Mr. BEYER. All right. Thank you, Mr. Gross. Thank you, Mr. Gibson.

Mr. Chairman, I yield back.

Chairman LOUDERMILK. I thank the Ranking Member for the line of questioning, and I thank the witnesses for their testimony and the other Members who were here with questions.

We've identified several inconsistencies here today by the FDIC, and the Committee will continue its oversight and looking forward to having the FDIC Chairman here once the Inspector General completes its audits. We will continue looking into this. This is a very critical issue.

And the record will remain open for two weeks for additional comment and written questions from the members.

The hearing is adjourned.

[Whereupon, at 11:40 a.m., the Subcommittee was adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Mr. Lawrence Gross, Jr.

ENCLOSURE

Acting Inspector General Fred Gibson's Response to Question for the Record

Question Submitted by Representative Don Beyer, Ranking Member Subcommittee on Oversight

QFR for Mr. Fred W. Gibson, Acting Inspector General, Federal Deposit Insurance Corporation (FDIC)

1) It is my understanding that the IG's office became part of the Data Breach Management Team in the wake of another cyber incident at FDIC in 2011 that the IG's office investigated in 2013 and was reported in *The Washington Post* on May 11, 2016. It is my understanding that in that case, senior officials in the CIO's office were not particularly forthcoming with either the FDIC Chairman, your office, or the Government Accountability Office about the circumstances of that penetration or the impact on the Agency.

    - Can you tell us what you can about this cyber incident and why the IG's office ended up being included in the Data Breach Management Team meetings in the wake of those cyberattacks?

Response: The cyber attacks to which the question refers involved the penetration of the FDIC's computer network by an "advanced persistent threat," or APT. In essence, an APT is an external actor that gains unauthorized access to a computer network, escalates its privileges, and develops an ongoing presence within the network at a level that permits the actor to compromise network, data, and component level security. In this case, the APT accessed numerous computers within the network over a significant period of time, including a computer used by the Chairman at the time and computers used by numerous other senior officials, and copied and exfiltrated large amounts of data from the network.

In 2010, the FDIC became aware of a significant intrusion and investigated it. The FDIC began investigating a second APT with similar characteristics in August 2011 but did not correlate the two threats at that time. The FDIC did not properly report the existence of the second APT to external authorities. The decision not to do so was made by the Chief Information Security Officer (CISO) at the time. The CISO also provided misleading responses to FDIC OIG auditors when they asked questions in connection with the 2011 and 2012 FISMA audits that should have revealed activity associated with the second APT. Similarly, the FDIC did not provide information about the APT to the Government Accountability Office (GAO) in connection with the GAO's annual financial statement audits of the Deposit Insurance Fund. Briefings to the current FDIC Chairman and other senior officials minimized the risks associated with the APT and left senior leadership with the significant misimpression that a minor incident had been contained. The former CISO retired shortly after we concluded our investigation.

ENCLOSURE

The FDIC took steps to assess and mitigate the APT in 2013. In addition, the FDIC modified its security governance structure by segregating the responsibilities of the Chief Information Officer from those of the Director of the Division of Information Technology, establishing a senior-level committee for assessing cyber security threats and developments impacting both the FDIC and the banking industry, and strengthening procedures to address future IT security incidents. Further, in 2013, the FDIC consolidated two existing committees to create the Data Breach Management Team (DBMT), which was designed to engage FDIC business function and process owners in the assessment of potential incidents to afford a more holistic view of operational and other risks and impacts. In our view, the identification, assessment, and mitigation of information security incidents is a program operating responsibility. The OIG was an earlier observer on the predecessor committees to the DBMT. Currently, the OIG frequently attends and observes DBMT meetings and reviews communications for awareness purposes in light of the OIG's mission to identify fraud and abuse, and to conduct investigations and audits relating to the operations of the FDIC.

Responses by Mr. Fred W. Gibson

Response to questions from
the Honorable Don Beyer
from the Federal Deposit Insurance Corporation

Q1: OMB Memorandum M-16-03 was released on October 30, 2015, and was very new guidance when FDIC was dealing with the aftermath of the October 2015 "Florida breach." The Memorandum laid out new responsibilities, new definitions, and new Congressional reporting deadlines for agencies hit with cybersecurity breaches.

a. Were you briefed on OMB Memorandum M-16-03 prior to your December 8th decision that the October breach was not a "major" incident?

b. If so, when was this briefing, who provided the briefing, who else was in attendance, and what specifically were you told about OMB Memorandum M-16-03?

c. What efforts, in detail, did the FDIC CIO office take in order to understand the dictates of OMB Memorandum M-16-03?

Evaluating incidents in light of the new OMB Memorandum M-16-03 was an immediate task for me when I started at the FDIC on November 2, 2015. The "Florida breach" activities, which occurred in September and October 2015 prior to my arrival and before OMB Memorandum M-16-03 was published, had been discovered on October 23, 2015. On October 30, 2015, the Friday before I arrived, M-16-03 was published. Although OMB Memorandum M-16-03 was published after the "Florida breach," I thought it appropriate that we consider whether or not the "Florida breach" would rise to the level of a "major" incident under OMB Memorandum M-16-03 guidance.

Since OMB Memorandum M-16-03 had just been issued, the FDIC had not yet updated policies and procedures to be responsive. I directed the CISO to compare OMB Memorandum M-16-03 with existing FDIC policies and procedures and to identify any changes required. I asked that target dates be identified for our policy and procedure revisions to address gaps within the FDIC IT management, privacy, and IT security programs.

Our Legal Division provided a written memorandum dated November 18, 2015, with the subject line "Applicability of OMB Memorandum M-16-03: Fiscal Year 2015-2016 Guidance on Improving Federal Information Security and Privacy Management Requirements." This memorandum provided background regarding FISMA applicability to the FDIC and related reporting requirements, and provided an overview of OMB Memorandum M-16-03. It also provided a section by section analysis of the memorandum that highlighted changes from prior guidance. I read this memorandum and understood the conclusion that "M-16-03 is generally applicable to the FDIC."

I sought input from the Chief Information Security Officer (CISO) and legal staff as we gathered and analyzed facts, and took risk mitigation steps consistent with our incident

handling policies and procedures in relation to the "Florida breach." Fact gathering and analysis is coordinated through a multi-disciplinary FDIC Data Breach Management Team (DBMT) that serves as an advisory body to the CIO when incidents occur. This multi-disciplinary advisory body reviews the information available to assess risk of harm to the FDIC and other entities. The DBMT also recommends actions to the CIO to mitigate the risk of harm. The DBMT met twice in November to consider the facts and recommend appropriate actions to be taken. The DBMT was cognizant of the new reporting requirements and recommended actions consistent with the guidance, such as counting the individuals whose PII was part of the incident.

Later, I also received an OIG memorandum dated February 19, 2016 with the subject line "Information Security Incident Warranting Congressional Reporting." I read the memorandum and understood the reasoning behind the OIG's interpretation of OMB Memorandum M-16-03 as it applied to the "Florida breach." We reported the "Florida breach" to Congress on February 26, 2016. I communicated to staff that we would use the OIG's interpretation going forward and in March we reported a late February incident using the OIG interpretation. In addition, we began a retroactive review of all incidents since October 30, 2015, through the present to determine if other previous incidents should be reported. We identified five additional incidents that we reported to Congress in May.

Q2: You've stated, in multiple mediums, that part of your rationale for originally NOT declaring the October 2015 breach a "major incident" was a host of "mitigating factors," including the belief that the former employee was not disgruntled, and the Agency's relationship with the employee was not adversarial.

a: Why did you find these "mitigating" factors dispositive in determining whether the breach was a "major incident"?

b: Who, if anyone, advised you that these factors were relevant or applicable to an assessment of a "major incident," and the ensuing reporting requirements, as described in OMB Memorandum M-16-03?

The facts surrounding the incident that were known at the time raised questions regarding whether or not the incident rose to the level of a "major" incident. In good faith, I considered, with input from the CISO and legal staff, the Federal Information Security Modernization Act of 2014 (FISMA 2014), OMB Memorandum M-16-03, and FDIC policies and procedures, which are based on NIST publications. Our intent was to follow the OMB Memorandum M-16-03 guidance, and to use FISMA 2014 and these other documents to provide context where we had questions as to OMB's intent.

I considered these mitigating factors (and others) in evaluating whether or not the breach was a major incident because I believed they were relevant to determining the risk of harm of the incident. I believed the four subparts of OMB Memorandum M-16-03's three-prong test existed to differentiate incidents where there was low risk of harm from those where there was greater risk of harm. Particularly, I believed these mitigating

factors were relevant to determining whether or not the information was recoverable, and whether or not it had been exfiltrated (two incident characteristics that are relevant to determining the risk of harm). Our internal Data Breach Handling Guide also instructs the reader to differentiate incidents based on risk of harm and points the reader to incident characteristics to consider.

In retrospect, and based on the OMB guidance and facts I had at the time, I should not have placed reliance on these factors in determining whether or not the incident was "major." After receiving the OIG's February 19, 2016 memorandum, we adopted their analysis and conclusions and have since then reported consistent with it. We would now classify a similar incident as major.

Q3: Can you tell us the total number of individuals and institutions affected by all seven of the breaches discussed at the hearing?

Our analysis to date indicates that approximately 200,000 individuals' information was involved in these incidents related to approximately 380 financial institutions. We are now in the process of offering credit monitoring services to the individuals at no cost to them to protect any individuals who were potentially affected, and to be responsive to the concerns raised by the members of the Committee.

Q4: Since the October OMB guidance has come out on major cyber incidents, has the issue of Congressional Notification been discussed at the Data Breach Management Team (DBMT) meetings?

Have you been party to any debate at the DBMT meetings or in any other settings at FDIC regarding Congressional Notification?

I have had a number of discussions with the DBMT collectively, and some members individually, to ensure members were aware of the heightened reporting obligations under FISMA 2014 and OMB Memorandum M-16-03. I had several discussions with the CISO, legal staff, and others as new information arrived. The notes from the DBMT's November 25, 2015 meeting indicate that the CISO also informed DBMT members of the FISMA reporting requirements. Finally, we recently had discussions regarding how our internal policies and procedures should be updated to better address FISMA 2014 and OMB Memorandum M-16-03. On June 13, 2016, we released version 1.5 of the guide that contained changes to reference the new reporting requirements in FISMA 2014 and OMB Memorandum M-16-03.

Q5: Have you discussed the new OMB guidance with other CIOs at other Executive Branch Agencies and specifically the issue of Congressional notification? Please summarize when and where these discussions took place and briefly describe the context of these discussions.

Soon after receiving the OIG's February 19, 2016 memorandum, I had informal telephonic discussions with my counterparts at other agencies to discuss the FDIC's reporting approach under FISMA 2014 and OMB Memorandum M-16-03.

Q6: In your testimony, you insinuated that not every breach with 10,000 or more affected records would trigger the 7-day Congressional notification requirement. (1698-1720) Under what authority do you make that assertion?

To clarify, although we have considered how best to update our policies and procedures to address FISMA 2014 and OMB Memorandum M-16-03, since receiving the OIG's February 19, 2016 memorandum, the FDIC has evaluated incidents consistent with the OIG's analysis and conclusions. For example, there was an incident in late February that was evaluated using the OIG's interpretation, which was reported to Congress in March. We have also reported five incidents based on a retrospective review of all incidents that occurred after October 30, 2015, but before receiving the OIG's memorandum.

OMB Memorandum M-16-03 guidance provides a three-prong test, two subparts of which specify the 10,000 or more record, or users affected count. One subpart implies that if the information in question is recoverable within a specified amount of time, and without supplemental resources, the 10,000 or more record, or users affected count, would not be applicable for that prong. In another subpart, if the incident does not involve the exfiltration, modification, deletion, unauthorized access, or lack of availability to information or systems, then that prong would not be triggered, regardless of the record, or users count.

I understand that the number of records and individuals potentially affected by an incident are significant factors in determining when to report to Congress, and also believe that there are types of incidents that should be reported before the number of records and individuals potentially affected is known, or when the number is known and under 10,000. An example would be an incident where an Advanced Persistent Threat actor is identified as having unauthorized network access, but it is not yet known whether records or individuals are affected.

Appendix II

Additional Material for the Record

DOCUMENTS SUBMITTED BY REPRESENTATIVE DARIN LAHOOD

FDIC

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500

Legal Division

December 2, 2015

By Email Redacted
and by Overnight Courier

Redacted

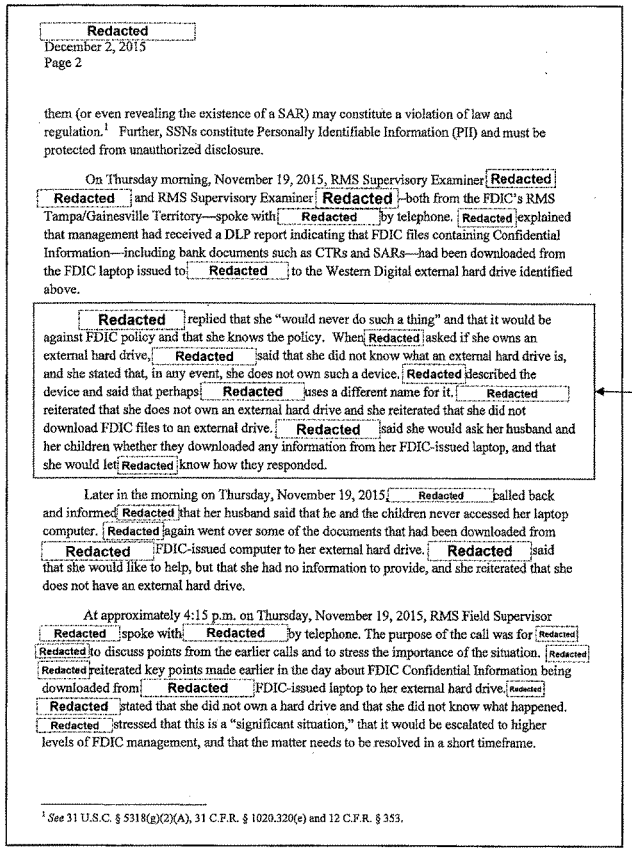
Re: Redacted Unauthorized Download of Confidential FDIC Information

Dear Redacted

We understand that you have been retained by Redacted to represent her in connection with inquiries that the Federal Deposition Insurance Corporation (FDIC) has made regarding Redacted unauthorized copying and removal of electronically-stored confidential or sensitive FDIC information (Confidential Information). As you may be aware, Redacted voluntarily resigned from her employment as a Bank Secrecy Act Specialist in the FDIC's Division of Risk Management Supervision (RMS) as of October 16, 2015. The FDIC subsequently discovered that in the weeks before her departure from the FDIC, she copied a large amount of Confidential Information and removed such Confidential Information from the FDIC's premises without appropriate authorization. This Confidential Information includes non-public bank supervisory information and other records belonging to the FDIC.

Specifically, through information obtained by the FDIC's Data Loss Prevention (DLP) program, we are aware that on September 16 and 17, and on October 15, 2015, Redacted downloaded large volumes of Confidential Information to an external drive that was not issued by the FDIC. The Security Event Logs from her laptop show that her user ID was the only account that logged on or unlocked the screen to her laptop on the identified dates. Forensic analysis indicates that the Confidential Information was downloaded to a Western Digital "My Passport Elite" 500 GB, USB 2.0 portable external drive, serial number Redacted

Forensic analysis further shows that the Confidential Information was downloaded to the identified portable external drive using a file naming convention that is consistent with the file naming convention that was previously used on Redacted FDIC-issued laptop. The Confidential Information includes social security numbers (SSNs), customer bank data, Suspicious Activity Reports (SAR) and Currency Transaction Reports (CTR) and logs from at least five financial institutions for which Redacted had supervisory responsibility. As Redacted is well aware from her work in the Bank Secrecy Act field, SARs and CTRs are highly confidential documents used for law enforcement purposes and improper disclosure of



Redacted
December 2, 2015
Page 2

them (or even revealing the existence of a SAR) may constitute a violation of law and regulation.[1] Further, SSNs constitute Personally Identifiable Information (PII) and must be protected from unauthorized disclosure.

On Thursday morning, November 19, 2015, RMS Supervisory Examiner Redacted Redacted and RMS Supervisory Examiner Redacted –both from the FDIC's RMS Tampa/Gainesville Territory—spoke with Redacted by telephone. Redacted explained that management had received a DLP report indicating that FDIC files containing Confidential Information—including bank documents such as CTRs and SARs—had been downloaded from the FDIC laptop issued to Redacted to the Western Digital external hard drive identified above.

Redacted replied that she "would never do such a thing" and that it would be against FDIC policy and that she knows the policy. When Redacted asked if she owns an external hard drive, Redacted said that she did not know what an external hard drive is, and she stated that, in any event, she does not own such a device. Redacted described the device and said that perhaps Redacted uses a different name for it. Redacted reiterated that she does not own an external hard drive and she reiterated that she did not download FDIC files to an external drive. Redacted said she would ask her husband and her children whether they downloaded any information from her FDIC-issued laptop, and that she would let Redacted know how they responded.

Later in the morning on Thursday, November 19, 2015, Redacted called back and informed Redacted that her husband said that he and the children never accessed her laptop computer. Redacted again went over some of the documents that had been downloaded from Redacted FDIC-issued computer to her external hard drive. Redacted said that she would like to help, but that she had no information to provide, and she reiterated that she does not have an external hard drive.

At approximately 4:15 p.m. on Thursday, November 19, 2015, RMS Field Supervisor Redacted spoke with Redacted by telephone. The purpose of the call was for Redacted Redacted to discuss points from the earlier calls and to stress the importance of the situation. Redacted Redacted reiterated key points made earlier in the day about FDIC Confidential Information being downloaded from Redacted FDIC-issued laptop to her external hard drive. Redacted Redacted stated that she did not own a hard drive and that she did not know what happened. Redacted stressed that this is a "significant situation," that it would be escalated to higher levels of FDIC management, and that the matter needs to be resolved in a short timeframe.

[1] *See* 31 U.S.C. § 5318(g)(2)(A), 31 C.F.R. § 1020.320(e) and 12 C.F.R. § 353.

[Redacted] replied that she "would never do such a thing" and that it would be against FDIC policy and that she knows the policy. When [Redacted] asked if she owns an external hard drive, [Redacted] said that she did not know what an external hard drive is, and she stated that, in any event, she does not own such a device. [Redacted] described the device and said that perhaps [Redacted] uses a different name for it. [Redacted] reiterated that she does not own an external drive and she reiterated that she did not download FDIC files to an external drive.

[redacted]

From: Toms, Roderick E.
Sent: Thursday, April 28, 2016 9:21 AM
To: Edwards, Serenity L.; Gross, Lawrence; Henning, Martin D.
Cc: Lowe, Richard
Subject: RE: Congressional Notification Memos: RMS Csirt Incidents Inc224419 and Inc221838 - > 10,000 Individuals Affected

Just to confirm –

We were notified of the 10K record count for these incidents on 4/27 so the 7 day reporting requirement will be 5/4.

Roderick Toms, PMP, CISSP

Acting Chief Information Security Officer
Information Security and Privacy Staff
FDIC
3501 N Fairfax Dr
Arlington, VA 22226

[redacted]

From: Edwards, Serenity L.
Sent: Wednesday, April 27, 2016 9:22 PM
To: Gross, Lawrence; Toms, Roderick E.; Henning, Martin D.
Cc: Lowe, Richard
Subject: Congressional Notification Memos: RMS Csirt Incidents Inc224419 and Inc221838 - > 10,000 Individuals Affected
Importance: High

Gentlemen,

Further to Rick's email to you, attached are the draft Congressional notification letters for CSIRT incidents INC224419 and INC221838, respectively. Please let me know if you have any questions.

Thank you,
Serenity

Serenity L. Edwards, CIPP/US, CIPP/G| Senior IT Specialist (Privacy) | Federal Deposit Insurance Corporation

[redacted]

From: Lowe, Richard
Sent: Wednesday, April 27, 2016 9:41 AM
To: Gross, Lawrence; Toms, Roderick E.
Cc: Henning, Martin D.

1

From: Roderick Toms
To: Larry Gross
Subject: Congressional Notification Memos: RMS Csirt Incidents Inc224419 and Inc221838.

We were notified of the 10k record count of these incidents on 4/27 so the 7 day reporting requirement will be 5/4.

Cybersecurity

DLP

10/23/2015 - CINC 221387 (Florida Incident)

DLP detected when a RMS Bank Secrecy Act Specialist (term employee) assigned to the Gainesville, Florida Field Office copieds approximately 1,200 files to a personally owned USB drive. ~~The copied files contained SSNs, Suspicious Activity Reports (SAR's) and Currency Transaction Reports (CTR's) related to at least five financial institutions (Colony Bank, Surety Bank, Englewood Bank, Davis Trust Company, and Burke & Herbert Bank). The files also contain former employee's personal information.~~

Status with date:

Open: Closed etc. If open ongoing actions

~~Update~~

~~RMS staff obtained the former employee's personally-owned device from her attorney. Another RMS employee hand-carried the device from Orlando to ISP staff at Virginia Square. ISPS Forensics now has the device and is in the process of analyzing it. ISPS Forensics has confirmed that this is the device that ISPS DLP software identified as receiving the three data downloads.~~

~~Timelins (week of 12/7 thru 12/11)~~

- ~~12/7/15 – FDIC Legal Staff contacted former employee's attorney. The former employee's attorney confirmed that he had the device that was used by the former employee to make downloads while she was employed at FDIC. FDIC Legal staff made arrangements with the attorney for FDIC RMS staff to obtain the device.~~
- ~~12/8/15 – RMS Staff visit attorney and obtain device.~~
- ~~12/9/15 – RMS Staff hand-deliver the device from Florida to Virginia Square building, where it is turned over to ISPS Forensics for inspection/review.~~
- ~~12/10/15 – FDIC Legal staff opine that ISPS Forensics may inspect/review non-FDIC owned device.~~
- ~~12/10/15 – ISPS Forensics begins inspection/review of device~~

12/4/2015 - CINC 222176

DLP detected that a recently departed employee Hill, Brooke R. copied Personally Identifiable Information (PII) to a USB Drive. The copied excel file contains 7000 Taxpayer ID numbers. The employee's last day seems to be 11/25/2015.

Status OPEN: Ongoing actions

Update

The USB used by recently departed employee, Brooke Hill, was issued by FDIC. Ms. Hill stated that her Field Office gave her permission to use the USB drive. The USB drive is in the possession of the Field Office Supervisor and will be turned-in to the DCP ISM on 12/14/15 for review and verification.

~~Timelins~~

- ~~Date DLP notified ISM: December 4, 2015 at 1:25pm~~
- ~~Date CSIRT Incident Created and Sent to ISM, etc.: December 4, 2015~~
- ~~Date ISM Spoke with Employee's Supervisor: December 4, 2015 at 2:18pm~~
- ~~Date Supervisor spoke with Employee: December 4, 2015~~
- ~~Date Employee turned in USB Drive to Supervisor: In Supervisor possession on 12/7. Will confirm once the Supervisor email Dale Witherspoon.~~