EVALUATING FDIC'S RESPONSE TO MAJOR DATA BREACHES: IS THE FDIC SAFEGUARDING CONSUMERS' BANKING INFORMATION?

HEARING

BEFORE THE

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

July 14, 2016

Serial No. 114–88

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
20–917PDF 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
WARREN DAVIDSON, Ohio

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

CONTENTS

July 14, 2016

EVALUATING FDIC'S RESPONSE TO MAJOR DATA BREACHES: IS THE FDIC SAFEGUARDING CONSUMERS' BANKING INFORMATION?

THURSDAY, JULY 14, 2016

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

The Committee met, pursuant to call, at 10:07 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Lamar Smith [Chairman of the Committee] 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

Full Committee

Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?

Thursday, July 14, 2016
10:00 a.m.
2318 Rayburn House Office Building

Witnesses

Mr. Martin Gruenberg, Chairman, FDIC

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

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

HEARING CHARTER

Tuesday, July 12, 2016

TO: Members, Committee on Science, Space, and Technology

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

SUBJECT: Full Committee hearing: *"Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?"*

The Committee on Science, Space, and Technology will hold a hearing titled *"Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?"* on Thursday, July 14, 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 major cybersecurity data breaches at the Federal Deposit Insurance Corporation (FDIC), and the agency's responses to these breaches pursuant to y the Federal Information Security Modernization Act of 2014 (FISMA).

The hearing will also examine the FDIC Office of Inspector General's release of two recent audit reports, which examine the FDIC's reporting of major security incidents to Congress, as well as the FDIC's controls for protecting sensitive resolution plans from unauthorized release.[1] The Committee will hear testimony from the Chairman of the FDIC as well as the FDIC Acting Inspector General about his office's recommendations for improving the FDIC's cybersecurity posture.

Witness List

- **The Honorable Martin J. Gruenberg**, *Chairman, FDIC*
- **Mr. Fred W. Gibson,** *Acting Inspector General, FDIC*

---

[1] Fed. Deposit Insurance Corp. Office of Inspector General, *The FDIC's Process for Identifying and Reporting Major Information Security Incidents* (Jul. 8, 2016) (AUD-16-004), *available at* https://www.fdicig.gov/reports16/16-004AUD.pdf (last visited Jul. 12, 2016); Fed. Deposit Insurance Corp. Office of Inspector General, *The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans* (Jul. 8, 2016) (AUD-16-003), *available at* https://www.fdicig.gov/reports16/16-003AUD.pdf (last visited Jul. 12, 2016).

Staff Contacts

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

Chairman SMITH. The Committee on Science, Space, and Technology will come to order.

Without objection, the Chair is authorized to declare recesses of the Committee at any time.

Welcome to today's hearing titled "Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?"

I'll recognize myself for an opening statement and then the Ranking Member.

The Acting Inspector General's recent audit confirms exactly what the Committee's ongoing investigation revealed: FDIC continues to have significant cybersecurity weaknesses.

Over the course of the Committee's bipartisan investigation, we have learned a great deal about the FDIC and how they conduct business. Yesterday we released an Interim Report by majority Committee staff.

The report contains the following findings: One: The FDIC has historically experienced deficiencies related to its cybersecurity posture, and those deficiencies continue to be present.

Two: The Chief Information Officer created a toxic work environment, misled Congress, and retaliated against whistleblowers.

Three: The FDIC deliberately evaded Congressional oversight.

The FDIC experienced at least eight major breaches that they have determined met the reporting guidelines issued by the Office of Management and Budget. The IG found that one of these breaches required law enforcement involvement. This was the September 2015, New York breach, in which a disgruntled employee, without authorization, downloaded sensitive resolution plans, also referred to as living wills. This breach, according to the IG's report and confirmed by a witness's testimony during our ongoing investigation, revealed that had the FDIC taken more than just the initial steps to implement a formal insider threat program, this breach could have been prevented or at the very least detected much earlier.

In a separate report, the IG found that the FDIC did not properly interpret and apply the reporting criteria required by a major incident, as articulated in the Office of Management and Budget memorandum. The OIG found that reasonable grounds existed to deem the Florida breach major but the FDIC waited four months to notify Congress.

The Committee is pleased that as a result of our hearing in May, the FDIC began the process of contacting individuals whose personally identifiable information had been compromised and offered them credit monitoring. The Committee also appreciates the fact that after nearly four months, the FDIC is working to produce all documents and communications that we have requested in multiple letters.

The agency initially produced redacted summaries of responsive documents and a limited set of email communications, but whistleblowers and the IG's staff immediately informed the Committee that we were not getting the whole story.

This has been the overreaching theme of the Committee's dealings with the FDIC: we're not getting the whole story. Based on

interviews and documents, there is a culture of concealment at the FDIC.

For example, the Office of Legislative Affairs staff, according to testimony, knowingly failed to provide the Committee with a full and complete production of documents.

The Office of General Counsel's staff directed their employees not to put certain opinions and analysis in emails or other written forms, presumably to avoid discovery through the Congressional oversight process.

This Committee takes seriously its cybersecurity responsibilities under the Federal Information Security Modernization Act of 2014, or FISMA, as well as our responsibility to root out waste, fraud, abuse, and mismanagement.

Our investigation has identified serious management deficiencies in the CIO's office. Certain FDIC employees believe that not only is he doing a poor job of protecting the agency's sensitive information technology, but also he's created a hostile work environment. One witness called Mr. Gross "vindictive," removing his staff from leading projects if they disagreed with his opinions.

The FDIC needs to be accountable for breaches of cybersecurity and responsive to the findings of our investigation.

We look forward to receiving all the requested documents and hearing about what steps the FDIC is taking to protect sensitive banking documents and taxpayers' personal information.

[The prepared statement of Chairman Smith follows:]

Statement of Science Committee Chairman Lamar Smith
Oversight Subcommittee Hearing on
Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?
10:00 a.m. Thursday, July 14, 2016

Thank you and thanks to our witnesses for being here today.

The Acting Inspector General's (IG) recent audit reports confirm exactly what the Committee's ongoing investigation revealed – FDIC continues to have significant cybersecurity weaknesses.

Over the course of the Committee's bipartisan investigation we have learned a great deal about the FDIC and how they conduct business. Yesterday we released an Interim Report by majority Committee staff. The Report contains the following findings:

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

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

3. The FDIC deliberately evaded congressional oversight.

The FDIC experienced at least eight major breaches that they have determined meet the reporting guidelines issued by the Office of Management and Budget.

The IG found that one of these breaches – the September 2015, New York breach, in which a disgruntled employee, without authorization, downloaded sensitive resolution plans, also referred to as living wills—required law enforcement involvement.

This breach, according to the IG's report and confirmed by witness testimony during our ongoing investigation, revealed that had the FDIC taken more than just the initial steps to implement a formal insider threat program, this breach could have been prevented and at the very least detected much earlier.

In a separate report the IG found that the FDIC did not properly interpret and apply the criteria for a major incident as articulated in the Office of Management and Budget Memorandum. The OIG found that reasonable grounds existed to deem the Florida breach major but the FDIC waited four months to notify Congress.

The Committee is pleased that as a result of our hearing in May, the FDIC began the process of contacting individuals whose personally identifiable information had been compromised and offered them credit monitoring.

The Committee also appreciates the fact that after nearly four months, the FDIC is working to produce all responsive documents and communications that we have requested in multiple letters.

The agency initially produced redacted summaries of responsive documents with a limited set of email communications. Thankfully, whistleblowers and the IG's staff immediately informed the Committee that we were not getting the whole story.

This has been the overreaching theme of the Committee's dealings with the FDIC – we're not getting the whole story. Based on interviews and documents, there is a culture of concealment at the FDIC. The Office of Legislative Affairs staff, according to testimony, decided not to provide the Committee with a full and complete production of documents.

The Office of General Counsel's staff directed their employees not to put certain opinions and analysis in email or other written form presumably to avoid discovery through the congressional oversight process.

This Committee takes seriously its cybersecurity responsibilities under the Federal Information Security Modernization Act of 2014, or FISMA, as well as our responsibility to root out waste, fraud, abuse, and mismanagement.

Our investigation has identified serious management deficiencies in the CIO's office. Certain FDIC employees believe that not only is he doing a poor job of protecting the agency's sensitive information technology, but also he's created a hostile work environment. One witness called Mr. Gross "vindictive," removing his staff from leading projects, if they disagreed with his opinions.

We look forward to your testimony today. I know you realize that the FDIC needs to be accountable for breaches as well as the results of our investigation.

We look forward to receiving all the requested documents and hearing about what steps FDIC is taking to protect sensitive banking documents and taxpayer's personal information.

###

Chairman SMITH. That concludes my opening statement, and the gentlewoman from Texas, Eddie Bernice Johnson, is recognized for hers.

Ms. JOHNSON. Thank you very much, Mr. Chairman, and welcome to our witnesses.

As we have learned over the course of many hearings before this Committee, cybersecurity is a never-ending struggle. Public and private entities alike are engaged in a constantly evolving challenge to prevent both intentional data breaches and unintentional dissemination of sensitive information.

Since the last hearing we held on data breaches at the Federal Deposit Insurance Corporation—the FDIC—just two months ago, 32 million Twitter users had their login credentials compromised, Walmart's corporate headquarters disclosed the unauthorized access to data of more than 27,000 customers, and the medical records of thousands of National Football League—the NFL—players were compromised when a laptop computer was stolen from a car.

Today is the Committee's second hearing on the FDIC's handling of several data breaches that occurred since October 2015 when the Office of Management and Budget—the OMB—issued new cybersecurity guidance. The OMB memo, known as Memo 16–03, helped to define what constitutes a major data breach and requires reporting incidents designated as major to Congress within seven days of such a determination. Data from the FDIC is particularly sensitive, and may include personal banking information and data indicating potential criminal activity such as suspicious activity reports.

The agency failed to notify Congress of seven major data breaches within the 7-day time frame that OMB requires from October 2015 through February 2016.

During our Oversight Subcommittee hearing on this topic in May, the FDIC's Chief Information Officer described these data breaches as inadvertent and occurring without malicious intent. The FDIC Acting Inspector General, Mr. Fred Gibson, testified at that hearing and is a witness here today. His office released two audits of the FDIC's data breaches last week, and the evidence his office gathered clearly shows that in at least one of the seven breaches, the data was not taken accidentally. His office is in the process of conducting a further forensic review of the remaining six incidences.

I think it's fair to say that our May hearing yielded bipartisan agreement that the FDIC's interpretation of the OMB guidelines was flawed. It is also clear that FDIC did not initially provide all documents responsive to the Committee's requests.

However, I do not agree with my Majority colleagues as to what constitutes evidence of intent. The Majority is likely to allege that the CIO intentionally misled the Committee and that the agency attempted to obstruct the Committee's investigation into these events. I do not believe the Committee has uncovered convincing evidence to support those allegations. I am not dismissing the testimony of some of the FDIC employees who have been interviewed but it is our responsibility to make sure we have all of the evidence and have heard from all parties before we begin to wave around serious allegations of criminal intent.

What I do believe is this. First, the recent reports issued by the Inspector General's office on the data breaches at FDIC point to a series of corrective actions that I hope will improve the agency's ability to appropriately respond to the multiple cybersecurity threats we all face. I do believe the FDIC Chairman takes these issues seriously. He has a strong track record on responding to cybersecurity challenges, including holding his staff accountable.

Second, all federal agencies need strong, competent, independent chief information officers—chief information security officers, and I am glad that both the IG's office as well as the Government Accountability Office, or GAO, are now engaged in separate reviews of the appropriate role, placement, and authorities of the Chief Information Security Officer at FDIC and other federal agencies.

And finally, while we investigate failures at different agencies to fully and properly implement federal cybersecurity requirements, we should also support agency efforts to continue to strengthen their cybersecurity posture as the technologies and the threats rapidly evolve around them.

I look forward to hearing from both Mr. Gruenberg and Acting IG Mr. Gibson.

Thank you, Mr. Chairman. 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
"Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?"
July 14, 2016

Thank you Mr. Chairman.

As we have learned over the course of many hearings before this Committee, cybersecurity is a never ending struggle. Public and private entities alike are engaged in a constantly evolving challenge to prevent both intentional data breaches and unintentional dissemination of sensitive information. Since the last hearing we held on data breaches at the Federal Deposit Insurance Corporation (FDIC), just two months ago, 32 million Twitter users had their login credentials compromised, Walmart's corporate headquarters disclosed the unauthorized access to data of more than 27,000 customers, and the medical records of thousands of National Football League (NFL) players were compromised when a laptop computer was stolen from a car.

Today is the Committee's second hearing on the FDIC's handling of several data breaches that occurred since October 2015 when the Office of Management and Budget (OMB) issued new cybersecurity guidance. The OMB memo, known as Memo 16-03, helped to define what constitutes a "major" data breach and requires reporting incidents designated as major to Congress within seven (7) days of such a determination. Data from the FDIC is particularly sensitive, and may include personal banking information and data indicating potential criminal activity, known as Suspicious Activity Reports.

The Agency failed to notify Congress of seven major data breaches within the seven-day timeframe that OMB requires from October 2015 through February 2016. During our Oversight Subcommittee hearing on this topic in May, the FDIC's Chief Information Officer (CIO), described these data breaches as "inadvertent" and occurring without "malicious intent." The FDIC Acting Inspector General Mr. Fred Gibson testified at that hearing and is a witness again today. His office released two audits of the FDIC's data breaches last week and the evidence his office gathered clearly shows that in at least one of the seven breaches the data was not taken accidentally. His office is in the process of conducting a further forensic review of the remaining 6 incidents.

I think it's fair to say that our May hearing yielded bipartisan agreement that the FDIC's interpretation of the OMB guidance was flawed. It is also clear that FDIC did not initially provide all documents responsive to the Committee's requests. However, I do not agree with my Majority colleagues as to what constitutes evidence of intent. The Majority is likely to allege that the CIO intentionally mislead this Committee and that the Agency attempted to obstruct the Committee's investigation into these events. I do not believe the Committee has uncovered convincing evidence to support those allegations. I am not dismissing the testimony of some of the FDIC employees who have been interviewed. But it is our responsibility to make sure we have all of the evidence and have heard from all parties before we begin to wave around serious allegations of criminal intent.

What I do believe is this:

First, the recent reports issued by the Inspector General's office on the data breaches at FDIC point to a series of corrective actions that I hope will improve the agency's ability to appropriately respond to the multiple cybersecurity threats we all face. I do believe the FDIC Chairman takes these issues seriously. He has a strong track record on responding to cybersecurity challenges, including holding his staff accountable.

Second, all federal agencies need a strong, competent and independent Chief Information Security Officer, and I am glad that both the IG's office as well as the Government Accountability Office (GAO) are now engaged in separate reviews about the appropriate role, placement, and authorities of the Chief Information Security Officer at FDIC and other federal agencies.

And finally, while we investigate failures at different agencies to fully and properly implement federal cybersecurity requirements, we should also support agency efforts to continue to strengthen their cybersecurity posture as the technologies and threats rapidly evolve around them.

I look forward to hearing from both Chairman Gruenberg and Acting IG Mr. Gibson.

I yield back.

Chairman SMITH. Thank you, Mrs. Johnson.

Let me introduce our witnesses. Our first witness today is Mr. Martin Gruenberg, Chairman of the Federal Deposit Insurance Corporation. Mr. Gruenberg previously served as Vice Chairman and Member of the FDIC Board of Directors. He was also Chairman of the Executive Council and President of the International Association of Deposit Insurers. Mr. Gruenberg received his bachelor's degree from Princeton University's Woodrow Wilson School of Public Policy and International Affairs and his J.D. from Case Western Reserve Law School.

Our second witness is Mr. Fred Gibson, Acting Inspector General of the Federal Deposit Insurance Corporation. Mr. Gibson previously has served with the Resolution Trust Corporation Office of Inspector General as Principal Deputy Inspector General and Council 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 also received his J.D. from the University of Texas School of Law.

We welcome you both, and Chairman Gruenberg, if you'll begin?

STATEMENT OF THE HON. MARTIN J. GRUENBERG, CHAIRMAN, FDIC

Mr. GRUENBERG. Thank you, Mr. Chairman. Chairman Smith, Ranking Member Johnson, and members of the Committee, thank you for the opportunity to appear before you today.

An effective information security and privacy program is critical to the FDIC's mission of maintaining stability and public confidence in the Nation's financial system.

My testimony today will discuss the recent incidents pertaining to information security at the FDIC and our response to the two related Office of Inspector General audits.

The first audit was of the FDIC's controls for mitigating the risk of an unauthorized release of sensitive resolution plans. As detailed in my written statement, on September 29, 2015, the FDIC determined through use of our Data Loss Prevention software that immediately prior to resignation, an employee in the FDIC's Office of Complex Financial Institutions had transferred copies of sensitive resolution plans from the internal network onto an unencrypted removable storage device, which was prohibited by FDIC policy. The FDIC notified the OIG of the incident on September 29, and law enforcement officials later recovered the storage device from the former employee. The OIG began an audit to determine the factors that contributed to this incident, and to assess the adequacy of mitigating controls.

Its final audit report identified several weaknesses that the FDIC needed to address and made six recommendations. We concur with the findings and recommendations, and expect to complete implementation of our responsive actions by the end of 2016. These include a recommendation that the FDIC establish an agency-wide insider threat program, which we have committed to fully implement by the end of this year. In addition, the OIG noted that a key control intended to prevent users from copying information to removable media failed to operate as intended. We are now installing

a new software version that addresses the observed defects and plan that installation to be completed by August 26.

The second audit I'd like to address is the OIG's audit of the FDIC's process for identifying and reporting major incidents, which stemmed from a breach of sensitive information that's referenced in the OIG report as the ″Florida Incident″. This incident involved a former FDIC employee who copied a large quantity of sensitive information to removable media and took the information when departing FDIC employment on October 15 of 2015. The FDIC detected the incident through its DLP software on October 23. The employee, who was initially resistant, ultimately returned the device on December 8 of last year.

Also during this time, on October 30 of last year, the Office of Management and Budget issued guidance on the reporting of ″major incidents″. In initially assessing the application of this new guidance and consistent with FDIC policy and procedure, the CIO considered the incident's risk of harm and reached the conclusion that although it was a breach, it did not rise to the level of a ″major incident″.

On February 19 of this year, the FDIC received an OIG memo analyzing the Florida incident in which the OIG concluded that the FDIC had not properly applied the OMG guidance for classifying the incident as a ″major incident″. The OIG found that the FDIC had based its determination on mitigating factors relating to ″risk of harm″, but that such factors are not addressed in the guidance and therefore are not relevant in determining whether or not incidents are major. The OIG determined that the FDIC should instead have reported the incident to Congress as a major incident no later than 7 days of having determined at least 10,000 Social Security Numbers were involved.

Having received this OIG memorandum, the FDIC proceeded to give Congressional notification on February 26 of this year. We then reviewed other incidents that had occurred since issuance of the guidance and reported six additional incidents to Congress between March and May.

In retrospect, and in light of the OIG's report findings, we should not have considered what we believed to be mitigating factors when applying the OMB guidance. We also failed to provide adequate context when reporting to Congress on the Florida incident and should have notified the potentially affected individuals when the notice to Congress was given in February.

We agree with the OIG conclusions and are working on each of their recommended corrective actions. Our expectation is that taking the steps outlined in the responses to the OIG reports will minimize the potential for similar incidents. I would note that the OIG's reports state that our planned actions are responsive and that the recommendations are resolved.

We have also discontinued the use of removable media at the FDIC except for limited exceptions for the GAO, OIG, and our legal division. We will keep the OIG and Congress informed of our progress.

Finally, if I may add, Mr. Chairman, there have been reports about advanced, persistent threat incidents in 2010 and 2011 at the FDIC. The Office of Inspector General provided me an inves-

tigative report back in May of 2013 on the incidents, which found that our Division of Information Technology did not fully inform me and other board members and senior executives about the incidents. As a result of that OIG report, we took a number of steps including engaging an independent cybersecurity firm to assist our system, and personnel changes were made.

Mr. Chairman, thank you again for the opportunity to testify today and I'd be happy to answer your questions.

[The prepared statement of Mr. Gruenberg follows:]

STATEMENT OF

MARTIN J. GRUENBERG
CHAIRMAN
FEDERAL DEPOSIT INSURANCE CORPORATION

on

INFORMATION SECURITY AT THE FDIC

before the

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

July 14, 2016
2318 Rayburn House Office Building

Chairman Smith, Ranking Member Johnson, and members of the Committee, thank you for the opportunity to testify before you today about the important issue of information security, including our efforts to identify and address information technology security incidents.

An effective FDIC information security and privacy program is critical to our mission of maintaining stability and public confidence in the nation's financial system. My testimony today will discuss the FDIC's cybersecurity posture, recent incidents pertaining to information security, and our response to the related Office of Inspector General audits.

The FDIC's Cybersecurity Posture

The National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity," dated February 12, 2014, is a product of the President's Executive Order[1] calling for the development of a voluntary risk-based cybersecurity framework to serve as industry standards and best practices for managing cybersecurity risks. The framework, created through collaboration between government and the private sector, adopts a common language to address and manage cybersecurity risk, and is the framework being used by the FDIC. The framework is composed of five functions: *Identify, Protect, Detect, Respond,* and *Recover.*

[1] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013.

1. Identify

The "Identify" function includes understanding the organization's business context, the resources that support its critical functions, and the related cybersecurity risks. Understanding these factors enables an organization to focus and prioritize its efforts, consistent with its risk-management strategy and business needs. In carrying out the "Identify" function, the FDIC seeks to explicitly identify our assets and characteristics useful in risk-mitigation activities. Our cyber assets include hardware, software, and data. We strive to keep accurate inventories of these assets and to categorize them from a risk standpoint so that higher-risk assets receive more attention when designing cybersecurity protections. For example, we have long maintained an inventory of our most sensitive data, including confidential bank examination reports, bank failure projections, and employees' sensitive personally identifiable information. We are currently updating that inventory and our process for maintaining it based on the Office of Management and Budget's (OMB) "high value asset" guidance.[2]

2. Protect

The "Protect" function of an organization's information security posture includes developing and implementing the appropriate safeguards to ensure delivery of critical infrastructure services. It speaks to an organization's ability to limit or contain the impact of a potential cybersecurity event. At the FDIC we have developed and implemented safeguards such as identity and access management, security awareness and training programs, data security

---

[2] Office of Management and Budget M-16-04.

protections, information protection processes and procedures, system maintenance routines, and protective technologies. In this function particularly, we strive for a "defense in depth" approach, so that if one safeguard fails, another will help us mitigate the potentially harmful impact of the failure. Our encryption of the hard drives of all of our examiners' laptops is a good example of a "Protect" activity. Also, as part of annual cybersecurity training required for all FDIC employees, we instruct our employees to be alert to anything that doesn't look right from an information security perspective ("see something/say something"). Periodic training exercises include mock email "phishing" campaigns. When an individual "fails" and clicks on an email link that should have seemed suspicious, they are immediately directed to a training page that identifies for them the email components that should have tipped them off. A final example of our activity in the "Protect" function is our recently adopted configuration of software to prevent an employee or contractor from copying information to removable media.

3. Detect

The "Detect" function of an organization's cybersecurity posture includes developing and implementing appropriate activities to identify the occurrence of a cybersecurity event. For example, logging various system actions allows us to monitor for anomalous activity. Another example of the many tools we use under the "Detect" function is the Data Loss Prevention or "DLP" software. DLP software monitors email traffic, uploads to websites, and printing for high-risk attributes that we have specified ahead of time. We review DLP reports for indications of activity inconsistent with our policies and procedures and take additional investigative steps when the circumstances warrant.

4. Respond

The "Respond" function of an organization's cybersecurity posture includes developing and implementing appropriate activities when a cybersecurity event is detected. For example, we have business continuity plans, which we revise periodically, that identify the steps we would take if a cybersecurity event rendered our primary datacenter inoperable. We also practice twice a year the failover of our mission critical systems to our backup datacenter. Another example of our "Respond" function is our data breach response program. We have an internal FDIC Computer Security Incident Response Team (CSIRT) that receives inputs from many different sources regarding events that could rise to the level of a breach. The team has procedures for escalating these events based on the risk of harm indicated by the event's characteristics. When events are escalated, an interdisciplinary team is convened and follows a data breach handling guide to determine what additional analysis steps are necessary, and what risk-mitigation activities should be pursued.

5. Recover

Finally, the "Recover" function of an organization's cybersecurity posture includes developing, implementing, and maintaining plans for restoring any capabilities or services that are impaired due to a cybersecurity event. The FDIC has disaster recovery plans that are reviewed periodically and would be followed in the event of a cybersecurity event that disabled our primary datacenter. We also practice through table top exercises what steps we would take to recover from a cybersecurity event, including the necessary communications with various counterparties and the public.

Recent Incidents and Related Audits

I would like next to address recent security incidents we experienced and two related audits by the FDIC Office of Inspector General (OIG). The first audit was of the FDIC's controls for mitigating the risk of an unauthorized release of sensitive resolution plans. The second audit was of the FDIC's process for identifying and reporting major incidents.

1. *Audit of the FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans*

   Background

   On September 29, 2015, the FDIC determined through use of its DLP software that an employee who had previously worked for the FDIC's Office of Complex Financial Institutions (OCFI) had transferred copies of sensitive resolution plans from the internal network onto an unencrypted removable storage device (or "thumb drive"). This activity violated OCFI policy, which prohibits the storage of resolution plans on removable media, and occurred immediately before the employee's resignation.

   The FDIC notified the OIG of the incident on September 29, and law enforcement officials later recovered the thumb drive containing the resolution plans, as well as a non-public executive summary of a resolution plan, from the former employee. As a result of this incident, the OIG commenced an audit, the objectives of which were to determine the factors that contributed to this security incident and to assess the adequacy of mitigating controls established following the incident.

OIG Recommendations and FDIC Responses

The OIG audit identified several weaknesses that the FDIC needed to address and made six recommendations. We concur with the OIG's findings and recommendations, and expect to complete implementation of all of our responsive actions by the end of 2016.

First, the OIG noted that an insider threat program would have better enabled the FDIC to deter, detect, and mitigate the risks by the employee. The OIG also noted that the FDIC has a number of long-standing controls designed to mitigate risks associated with trusted insiders, including background investigations, periodic inspections of FDIC facilities to identify security concerns, employee nondisclosure agreements, a DLP tool, and programs to help employees with personal issues.

In 2014 and 2015, the FDIC began to take steps toward establishing a formal insider threat program by developing draft governance, policy, and procedures, and by initiating interdivisional discussions on the topic. However, as of October 2015, the insider threat program had not been implemented.

An insider threat program is a program designed to prevent, detect, and respond to threats from malicious insiders. A malicious insider is a current or former employee, contractor, or business partner who has, or had, authorized access to an organization's network, systems, or data, and has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. An insider threat program would analyze information sources to identify situations that appear to present higher risk levels so that appropriate action can be taken.

The OIG recommended that the FDIC establish an agency-wide insider threat program that is consistent with NIST-recommended practices and applicable laws, executive orders, national strategies, directives, regulations, policies, standards, and guidelines. In response, we have committed to fully implement such an insider threat program, building significantly on certain elements that are already in place. A team of executive-level staff will finalize the FDIC's insider threat program policy statement and governance structure by October 28, 2016; an insider threat working group is being established to carry out the program by October 28, 2016; and appropriate employee awareness and training efforts will be completed by December 30, 2016.

Second, the OIG noted that a key control intended to prevent the copying of sensitive resolution plans to removable media did not function properly.

The OIG recommended that the FDIC Chief Information Officer (CIO) immediately test the effectiveness of the control designed to prohibit network users from copying information to removable media to confirm that the control operates as intended. Between October 2015 and April 2016, the FDIC's Division of Information Technology coordinated tests with OCFI and others to ensure the software that prohibits copying files to removable media was working properly. While the majority of the tests were successful, some tests identified defects in limited situations. We are now installing a new software version that addresses the observed defects and plan that installation to be completed by August 26, 2016. Documentation of the test steps and the results of the test will be improved. In addition, we will develop a comprehensive test plan and use it to regularly re-evaluate the effectiveness of the software that prohibits users from copying information to removable media.

Third, the OIG recommended that the CIO coordinate with other FDIC division and office directors to revise and/or develop written policies and procedures, as appropriate, to govern the control designed to prohibit network users from copying information to removable media. In response, by the end of September the CIO organization will coordinate with division and office directors to identify and update relevant directives and procedures to ensure consistency with the FDIC's general decision to prohibit any copying of information to removable media. This will include protocols for managing any limited exceptions to the general prohibition and a requirement for regular testing of the software control's effectiveness.

Fourth, the OIG recommended that the Director of OCFI assign a dedicated information security manager (ISM) to support OCFI, given OCFI's regular handling of sensitive resolution plans. In response, OCFI will work with FDIC human resources staff to announce and by year-end fill a position for an ISM dedicated solely to OCFI.

Fifth, the OIG recommended that the Director of OCFI evaluate whether employees should continue to be allowed to store copies of sensitive resolution plans outside of the special secure OCFI system (referred to as ODM) designed for such plans. In response, OCFI is in the process of updating its policy to prohibit the practice of storing resolution plans outside of ODM (even if certain other locations may be considered secure) and to address controls on printing and downloads of resolution plans. This updating will be completed by the end of September.

Sixth, the OIG recommended that the Director of OCFI develop appropriate policies and procedures addressing the new and enhanced security controls that had been established by OCFI following the incident in question and periodically assess the effectiveness of such controls. In

response, OCFI is in the process of revising its policies and procedures to address the new and enhanced security controls, and plans to complete that work by the end of September. Particularly, OCFI will develop comprehensive procedures incorporating control activities to mitigate program risks and ensure that resolution plans are adequately safeguarded, including plans for periodic testing to ensure that the controls are repeatable, consistent, disciplined, and operating as intended.

In summary, the FDIC controls intended to protect resolution plans did not work with regard to the incident in question. This is a serious matter that must be addressed so that it does not happen again. The OIG's review has been helpful to us in identifying the necessary corrective actions, and we will diligently complete them.

The second audit I would like to address is the OIG's Audit of the FDIC's Process for Identifying and Reporting Major Incidents.

2. *Audit of the FDIC's Process for Identifying and Reporting Major Incidents*

Background

This audit stemmed from a breach of sensitive information that is referenced in the OIG report as the "Florida Incident." This incident involved a former FDIC employee who copied a large quantity of sensitive FDIC information, including personally identifiable information of bank customers, to removable media. The employee took the information when the employee left the FDIC on October 15, 2015. The FDIC detected the incident through its DLP software on October 23 and notified the CSIRT. The individual's former supervisor initially contacted the

individual on October 26, 2015. On November 2, 2015, the current Chief Information Officer arrived at the FDIC. On November 6, the FDIC requested assistance from the OIG's Office of Investigations (OI) to resolve the incident and OIG initiated a request that same day for additional information. On November 19, 2015, and December 2, 2015, the FDIC again had contact with the employee who was initially resistant but ultimately returned the device on December 8, 2015.

Also during this time period, on October 30, 2015, OMB issued its Memorandum M-16-03, which provides federal agencies with guidance on the reporting of "major incidents." Although OMB Memorandum M-16-03 was received after the incident occurred, the guidance nonetheless was considered and applied as part of the FDIC's ongoing response to the incident. In initially assessing the application of this new guidance, and consistent with existing FDIC policy and procedure, the CIO considered the incident's risk of harm and reached the conclusion that although it was a breach, it did not rise to the level of a "major incident."

On February 19, 2016, the FDIC received an OIG memorandum containing analysis of the Florida Incident in which the OIG concluded that the FDIC had not properly applied the OMB guidance for classifying the incident as a "major incident."[3] The OIG found that the FDIC had based its determination that the Florida Incident was not a major incident on various mitigating factors related to "risk of harm" posed by the incident, but that such factors are not addressed in M-16-03 and therefore are not relevant in determining whether incidents are major. The OIG determined that the FDIC should instead have reported the Florida Incident to Congress

[3] OMB M-16-03.

as a major incident no later than seven days after it was determined that more than 10,000 unique Social Security numbers were involved in the breach.

We received this OIG memorandum regarding congressional notification on February 19, 2016, while the OIG's audit was still ongoing. We then proceeded to give such notification on February 26, 2016. We also reviewed other incidents that had occurred since issuance of M-16-03 and reported six additional incidents to Congress between March and May 2016.

The OIG also concluded that when the FDIC notified Congress of this incident, the notifications were inadequate. Particularly, the OIG stated that the notifications did not accurately portray the extent of risk associated with the Florida Incident.

In retrospect, and in light of the OIG's report findings, we should not have considered what we believed to be mitigating factors when applying the OMB guidelines. Having carefully reviewed the OIG audit, we agree with the OIG's conclusions and are working on each of the recommended corrective actions, as outlined below.

OIG Recommendations and FDIC Responses

The OIG final audit stemming from the Florida Incident identified several weaknesses that the FDIC needed to address and made five recommendations. We concur with the OIG's findings and recommendations and expect to complete implementation of all of our responsive actions by the end of 2016.

First, the OIG report notes that FDIC incident response policies, procedures, and guidelines did not address major incidents and recommends that the CIO revise the FDIC's

incident response policies, procedures, and guidelines to address major incidents. In response, we are revising our incident response policies and other relevant documents as indicated. The CIO has already issued an interim update of our Data Breach Handling Guide to explicitly refer the reader to FISMA and M-16-03 as the operative guidelines for what constitutes a major incident for congressional reporting purposes. Further, a more comprehensive review and revision process is underway with respect to the Data Breach Handling Guide and other relevant FDIC policy and procedure documents to refine roles and responsibilities for designating incidents appropriately and to ensure incidents are appropriately escalated for action, including timeliness of decision-making and congressional notification. This comprehensive review and revision will be completed by the end of September 2016.

Second, the OIG report notes that the FDIC's DLP tool can be better leveraged to identify major incidents. The OIG recommended that the CIO review our current implementation to determine how the tool can be better leveraged to safeguard sensitive FDIC information. We agree and will review its current implementation by year-end. We will consider data classification standards guidance in assessing DLP tool keywords and filters, and will follow a project plan that identifies approved tasks resulting from the DLP review.

Third, the OIG report notes that the FDIC did not properly apply OMB guidelines in its evaluation and reporting of the Florida Incident. The OIG recommends that the CIO ensure that revisions to the FDIC's incident response policies and procedures include criteria for determining whether an incident is major, consistent with FISMA and M-16-03.

It is important that any determination of whether an incident is major be made consistent with FISMA and M-16-03. As noted above, we have published an interim update to our Data Breach Handling Guide that directs the reader to FISMA and M-16-03 to consider when external incident notification steps are required. We will further edit policies and procedures to ensure that they are clear with respect to the criteria that should be applied for determining when an incident is major, consistent with FISMA and with M-16-03, by September 30, 2016. To ensure ongoing consistency between FDIC policy and procedure and OMB guidance, we will also review FDIC policies and procedures periodically in light of any relevant OMB revisions or other guidance obtained from OMB.

Fourth, the OIG report notes that the FDIC congressional notifications did not accurately portray the extent of risk associated with the Florida Incident. The OIG recommended that the CIO establish controls to ensure that future congressional notifications of major incidents include appropriate context regarding risks associated with such incidents and that statements of risk are supported by sufficient, appropriate evidence.

It is important that FDIC congressional notifications of major incidents include appropriate context regarding the risks associated with the incidents. In response, the CIO has already issued a memorandum to his staff implementing this recommendation. The memo stresses the importance of including appropriate context in any notifications of major incidents, including the supportability of any statements of risk. The issue of appropriate context will also be taken into account in our other reviews of policies and procedures being undertaken in response to the OIG's two audits.

Fifth, as the OIG report notes, management of incident investigative records and related documentation needs improvement. The OIG recommended that the CIO review and update, as appropriate, incident response policies, procedures, and guidelines to require proper recording and central maintenance of documentation relating to investigations and decision-making.

We agree that incident documentation should be managed centrally; that it should be kept current, accurate, and complete; and that it should contain the underlying analysis for key decisions and discussions. Our review and updating of various policies and procedures as referred to previously will take these points into account and will be completed by the end of September.

As a final note with respect to both audits, it is worth noting that the FDIC has discontinued individuals' ability to copy information to removable media such as external hard drives, flash drives, and CDs or DVDs to prevent these types of incidents from occurring in the future. Exceptions are currently limited to on-site Government Accountability Office employees, OIG staff, and a few FDIC legal technical staff as necessary for litigation, FOIA, or congressional requests that may necessitate removable media usage.

Conclusion

As I indicated at the outset, information security is critical to the FDIC's ability to carry out its mission of maintaining stability and public confidence in the nation's financial system. Our expectation is that by taking the steps outlined we will be effective in significantly minimizing the potential for similar incidents going forward. I would note that the OIG's final

reports state that our planned actions are responsive to the recommendations and the recommendations are resolved. We will keep the OIG and Congress informed of our progress.

Thank you again for the opportunity to testify today. I would be happy to answer your questions.

Martin J. Gruenberg

Martin J. Gruenberg is the 20th Chairman of the FDIC, receiving Senate confirmation on November 15, 2012 for a five-year term. Mr. Gruenberg served as Vice Chairman and Member of the FDIC Board of Directors from August 22, 2005 until his confirmation as Chairman. He served as Acting Chairman from July 9, 2011 to November 15, 2012, and also from November 16, 2005 to June 26, 2006.

Mr. Gruenberg joined the FDIC Board after broad congressional experience in the financial services and regulatory areas. He served as Senior Counsel to Senator Paul S. Sarbanes (D-MD) on the staff of the Senate Committee on Banking, Housing, and Urban Affairs from 1993 to 2005. Mr. Gruenberg advised the Senator on issues of domestic and international financial regulation, monetary policy and trade. He also served as Staff Director of the Banking Committee's Subcommittee on International Finance and Monetary Policy from 1987 to 1992. Major legislation in which Mr. Gruenberg played an active role during his service on the Committee includes the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA); the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA); the Gramm-Leach-Bliley Act; and the Sarbanes-Oxley Act of 2002.

Mr. Gruenberg served as Chairman of the Executive Council and President of the International Association of Deposit Insurers (IADI) from November 2007 to November 2012.

Mr. Gruenberg holds a J.D. from Case Western Reserve Law School and an A.B. from Princeton University, Woodrow Wilson School of Public and International Affairs.

Chairman SMITH. Thank you, Chairman Gruenberg.
And Mr. Gibson.

**STATEMENT OF MR. FRED W. GIBSON,
ACTING INSPECTOR GENERAL, FDIC**

Mr. GIBSON. Thank you, Chairman Smith, Ranking Member Johnson, Members of the Committee. Thank you for the invitation to speak with you today.

Since I last testified before this Committee's Subcommittee on Oversight, my office has completed two publicly available audits relating to the information security posture of the FDIC. Our first audit dealt with the FDIC's process for identifying and reporting major incidents and focused on the reporting of one such incident, which is being referred to as the Florida incident.

This incident involved a former FDIC employee who copied a large quantity of sensitive FDIC information to removable media and took this information when the employee left in October of 2015. The FDIC detected the incident through its data loss prevention tool. We determined that although the FDIC had established various incident response policies, procedures, guidelines, and processes, these controls did not provide reasonable assurance that major incidents were identified and reported in a timely manner consistent with the law and OMB guidance. We made five recommendations that were intended to provide the FDIC with greater assurance that major incidents are accurately identified and promptly reported

Our analysis of the Florida incident prompted the FDIC to initiate a review of similar incidents involving departing employees that occurred after the OMB issued applicable guidance in October of 2015. Based on its review between March and May 2016, the FDIC reported six additional incidents to the Congress as major. We are currently studying these incidents and the manner in which they were reported and expect to complete this work by mid-September.

In a second audit, we reviewed the Corporation's controls for mitigating the risk of an unauthorized release of sensitive resolution plans. Under Dodd-Frank, designated systemically important institutions must provide resolution plans to federal bank regulators. These resolution plans, or living wills, contain some of the most sensitive information that the FDIC maintains.

In September 2015, an FDIC employee working in the FDIC's Office of Complex Financial Institutions abruptly resigned from the Corporation and took copies of non-public components of resolution plans without authorization and in violation of FDIC's policies. The incident is not one of the seven that the FDIC reported as major to the Congress. Our work identified a number of factors contributing to the security incident. We concluded that an Insider Threat program would have better enabled the FDIC to deter, detect and mitigate the risk of an event like this, and a key security control designed to prevent employees with access to sensitive resolution plans from copying electronic information to removable media had failed to operate as it was intended. Our report contains six recommendations. One is that the FDIC establish a corporate-wide Insider Threat program.

The FDIC concurred with the recommendations we made in both audits and has outlined actions that would be responsive. We will follow up carefully on the implementation of each of those recommendations.

We will also complete this year's FISMA audit in the fall. The report will build upon the work I've described today and will broadly assess the effectiveness of the FDIC's information security program and practices.

In addition, we have ongoing work related to the FDIC's plans and actions to address earlier audit recommendations pertaining to credentialing and multifactor authentication. We plan to initiate additional audit work in such areas as data breach notification and the FDIC's information technology enterprise architecture.

Finally, we also have open investigations relating to several of these matters, which have not reached the stage where further public discussion would be appropriate.

In any case, thank you again. I look forward to answering any questions the Committee may have about these or any related matters.

[The prepared statement of Mr. Gibson follows:]

Testimony

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

The Federal Deposit Insurance Corporation's Information Security Posture

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

July 14, 2016

Statement of Fred W. Gibson, Jr.
Acting Inspector General, Federal Deposit Insurance Corporation
July 14, 2016

Chairman Smith, Ranking Member Johnson, and Members of the Committee,

Thank you for the invitation to speak with the Committee today. Since I last testified before this Committee's Subcommittee on Oversight, my office has completed two audits relevant to the information security posture of the FDIC that are now publicly available, and we are conducting additional work related to the FDIC's information security program controls, including incident handling.

MAJOR SECURITY INCIDENTS

Our first audit dealt with the FDIC's process for identifying and reporting major information security incidents and focused on one such incident (referred to as the Florida Incident). This incident involved a former FDIC employee who copied a large quantity of sensitive FDIC information, including personally identifiable information, to removable media and took this information when the employee departed the FDIC's employment in October 2015. The FDIC detected the incident through its Data Loss Prevention tool.

We determined that although the FDIC had established various incident response policies, procedures, guidelines, and processes, these controls did not provide reasonable assurance that major incidents were identified and reported in a timely manner. Specifically, we found that:

- The FDIC's policies, procedures, and guidelines did not address major incidents.
- The FDIC's Data Loss Prevention tool and related processes could be better leveraged to identify major incidents.
- The FDIC did not properly apply Office of Management and Budget (OMB) guidance in Memorandum M-16-03 when evaluating the Florida Incident.
- Congressional notification letters related to the Florida Incident included risk mitigation factors that were either unsupported by adequate evidence and/or inconsistent with information available at the time. As a result, in our view, the notifications did not accurately portray the extent of risk associated with the incident.
- Key decisions pertaining to the Florida Incident were untimely, and a required notification to another federal agency was not made.
- Management of investigative records and related documentation needed improvement.

We made five recommendations intended to provide the FDIC with greater assurance that major incidents are identified and reported consistent with the Federal Information Security Modernization Act of 2014 and OMB guidance. FDIC management concurred with all five recommendations and is taking responsive actions.

The results of our analysis of the Florida Incident prompted the FDIC's Chief Information Officer to initiate a review of similarly-situated incidents that occurred after the OMB issued Memorandum M-16-03 to determine whether additional incidents warranted designation as major. The FDIC reported six additional incidents to the Congress as major between March and May 2016. We are currently conducting a review of the six incidents and the manner in which they were reported to the Congress and expect to complete this work by mid-September.

SENSITIVE RESOLUTION PLANS

In a second audit, we reviewed the Corporation's controls for mitigating the risk of an unauthorized release of sensitive resolution plans.

Under the Dodd-Frank Wall Street Reform and Consumer Protection Act, certain financial companies designated as systemically important must report to the FDIC on their plans for a rapid and orderly resolution under the Bankruptcy Code in the event of material financial distress or failure. These resolution plans or living wills contain some of the most sensitive information that the FDIC maintains. Safeguarding the plans from unauthorized access or disclosure is critically important to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system.

In September 2015, an FDIC employee working in the FDIC's Office of Complex Financial Institutions abruptly resigned from the Corporation and took copies of sensitive components of resolution plans without authorization and in violation of FDIC policy. This incident is not one of the seven that the FDIC reported as major to the Congress.

Our work identified a number of factors contributing to this security incident. Most notably:

- An insider threat program would have better enabled the FDIC to deter, detect, and mitigate the risks posed by the employee.
- A key security control designed to prevent employees with access to sensitive resolution plans from copying electronic information to removable media failed to operate as intended.

The remaining factors involved OCFI employees having access to resolution plans that exceeded business needs; OCFI's inability to effectively review and revoke employee access to resolution plans because employees were allowed to store copies of the plans outside of the FDIC's official system of record—OCFI Documentum (ODM); and OCFI's inability to monitor all downloading of resolution plans stored in ODM.

Our report contains six recommendations. Specifically, we recommended that the FDIC establish a corporate-wide insider threat program. The remaining five recommendations are intended to strengthen the FDIC's information security controls, particularly with respect to safeguarding sensitive resolution plans submitted to the Corporation under the Dodd-Frank Act.

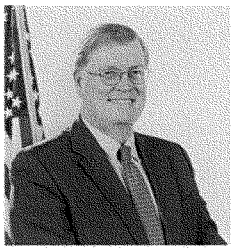
The FDIC has outlined actions that are responsive to the recommendations in our report, and we will follow up on the implementation of those recommendations, as appropriate.

ONGOING WORK

In addition to our ongoing work with regard to the six reported incidents, we will complete this year's FISMA audit in the fall. The report will build upon the work I have described today and will broadly assess the effectiveness of the FDIC's information security program and practices. In addition, we have ongoing work related to the FDIC's plans and actions to address prior recommendations that we made pertaining to credentialing and multifactor authentication. We plan to initiate additional work in such areas as data breach notifications and the FDIC's information technology enterprise architecture.

Finally, we also have open criminal investigations relating to several of the incidents, which have not reached a stage where further public discussion would be appropriate.

Thank you, again. I look forward to answering any questions the Committee may have about these or related matters.



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 SMITH. Thank you, Mr. Gibson, and I'll recognize myself for questions.

Chairman Gruenberg, let me address my first one to you and say that it's our understanding that no staff has been reprimanded for mishandling the cybersecurity breaches, no staff has been reassigned because of the mishandling of breaches, and the appearance is that no one's been held accountable for the breaches. I am just wondering why not.

Mr. GRUENBERG. Thank you, Mr. Chairman. If I may, let me give you my perspective on this, particularly in regard to our CIO, who I think has been the lead person responsible in this are. I understand this may not be consistent with your perspective but I wanted to give you my perspective for what it's worth from my position. As you know, the incident that precipitated this, the Florida, so-called ″Florida Incident″, occurred on October 15, and was identified on October 23, and the OMB guidance on major incident was issued on October 30, and our CIO began—assumed his responsibilities on November 2. So what we had was sort of a confluence of developments. The breach occurred and was identified, the guidance was issued, and our CIO assumed his new position. It was sort of presented, if I may say, with a pretty—for a guy just starting the job—a pretty difficult situation to sort through. He had the breach occur. He had to—the decision was made that even though the breach occurred before the issuance of the guidance there'd be an effort made to apply the guidance to the breach, but it was new guidance, first impression without real precedent to go by.

Chairman SMITH. Right. Let me interrupt you just briefly.

You had six major breaches. One was so serious it involved law enforcement, and there were a number of individuals involved, not just the one CIO, but it appears that again no reprimands, no reassignments, no accountability for anyone, and that sends a message that the breaches are not necessarily being taken seriously.

Mr. GRUENBERG. Mr. Chairman, I assure you we have no higher priority at the FDIC than addressing these matters. We certainly are prepared to consider the information provided by the Committee and review and consider them in regard to the——

Chairman SMITH. And this particular breach was not reported to the Committee for four months. Was there any good explanation why the FDIC waited to report the incident?

Mr. GRUENBERG. This is in regard to the Florida incident?

Chairman SMITH. The Florida incident. Correct.

Mr. GRUENBERG. If I could just complete my comments on that.

The CIO, who is the responsible official, was trying to sort through the application of the new guidance to this incident. He utilized existing FDIC policy of considering the risk of harm, applying the guidance, and utilizing mitigating factors applying to risk of harm, and a conclusion was reached that that incident was a breach that would be reportable under FISMA, but did not rise to the level of a ″major incident″. That was the assessment made based on the facts available to the CIO.

That occurred in December. When the OIG, who then was reviewing this matter, provided a memo in February, on February 19 saying no, you got it wrong, these mitigating factors are not provided in the guidance, they're not relevant——

Chairman SMITH. There was a difference of opinion as to how you define "major"?

Mr. GRUENBERG. That's really what it came down to, and I guess what I want to suggest, and I understand there may be a difference of view. While we may have gotten it wrong, while the CIO may have gotten it wrong, I think, at least my perspective is, there was an honest effort here to review the guidance, consider mitigating factors, and make a reasonable judgment. The judgment may have been wrong, but I don't think there was malintent here. That's what I wanted to convey.

Chairman SMITH. Thank you, Chairman Gruenberg.

And Mr. Gibson, are you satisfied that the FDIC are taking the necessary steps or will take the necessary steps to address your findings?

Mr. GIBSON. Sir, in our view, the FDIC has described actions that if taken will be responsive to the recommendations of each one of our audits. I mean, it's our intention to follow up with respect to the implementation of each one in order to ensure both that they're implemented and that it's done so in an effective manner and that the effect of those actions achieves the goal that we were trying to achieve.

Chairman SMITH. Okay. Thank you, Mr. Gibson.

I'll recognize the Ranking Member, Eddie Bernice Johnson, for her questions, but let me say that I'm going to need to shuttle between this Committee hearing and another committee hearing, so I'm going to turn the chair over to the gentleman from Georgia, Mr. Loudermilk, and hope to return.

The gentlewoman from Texas is recognized for her questions.

Ms. JOHNSON. Thank you, Mr. Chairman.

Chairman Gruenberg, several years ago before the current CIO came to the agency, the FDIC suffered from a cyber-attack by a foreign government. I understand that a senior IT security staff member failed to inform you about this breach at the time. Once you found out about it, I also understand that you took disciplinary actions against some of these individuals who failed to inform you of this breach.

The FDIC IG's office says that in one of the recent data breaches, known as the Florida Incident, your Chief of Information Officer decided not to forward information to you about the breach because he made the determination it was not a major incident and therefore did not need to pass this along for your approval.

Given this history, are you taking any specific steps to ensure that you are being kept well-informed of cybersecurity issues at your agency?

Mr. GRUENBERG. Thank you, Congresswoman. We are, needless to say, very focused on this set of issues. As I indicated, they are critical and essential to the functioning and credibility of our agency, and we are engaging on a daily basis in terms of complying with all of the recommendations and implementing all of the recommendations made by the OIG including implementing policies and procedures relating to major incidents that will assure the timely reporting to Congress if such incidents should occur again.

Ms. JOHNSON. Thank you.

Mr. Gibson, I understand that your office is undertaking review of the role of the Chief Information Security Officer to make sure that he or she has the authorities and independence necessary to ensure a strong cybersecurity posture for the agency. I know that this review is just getting started, but can you tell us what sorts of questions you are trying to address and why you're conducting this in the first place?

Mr. GIBSON. Yes, ma'am. We believe that the Chief Information Security Officer as a matter of principle should be in a position to speak up and in a position to inform those in the corporation who need to know what the status is of incidents of information that may be relevant pertaining to the security of the system. I'm not sure that we have reached—we obviously haven't reached any conclusions yet but the goal is essentially to reach a reasoned assessment as to whether the CISO in current structure where the CISO reports to the Chief Information Officer is able to provide that independent, security-minded voice with respect to that information or whether it's a position that should organizationally and from a governance standpoint be separated so that there's a degree of independence and a degree of ability to speak up.

Ms. JOHNSON. Now, in regards to the seven data breaches reported to Congress by the FDIC as major incidences, do you believe that the circumstances in those specific cases gave the agency the discretion to determine that they were not major incidences as they initially were determined?

Mr. GIBSON. We're still reviewing all six of those incidents so our work isn't complete. What I would say at this point in time preliminarily is we believe they should all have been reported as major incidents consistent with 16-03.

Ms. JOHNSON. Thank you very much.

I yield back.

Mr. LOUDERMILK. [Presiding] I thank the lady from Texas, and now recognize myself for five minutes for questions.

Mr. Gruenberg, you had mentioned earlier that Mr. Gross was assessing the risk of harm as one of the reasons that it wasn't reported to Congress. I may remind you that risk of harm is not one of the criteria in OMB. It's the scope and the type of documents which I think is clearly in the realm of what should have been reported and reported within seven days, not in several months, but it's not the place of this Committee to try to micromanage the operations within FDIC, but when the operations puts at risk the safety and security of American citizens or our national security, then it is our responsibility, it's our duty to inject ourselves on behalf of the American people.

And so in our previous hearing, we really looked at in depth, as in depth we could, as to what happened in those data breaches. Today I want to assess what is the response. Because I think it's important that we understand the direction that you're taking. Is it effective? Are we actually trying to correct that as we go forward in still investigating what happened and why the law was not followed? We also need to know what direction you're going.

Now, I understand that through testimony before that you have a data loss-prevention program, DLP, that is, I believe, a Symantec program, that actually notified the FDIC and your data team that

this data had been copied, and so that kind of prompted your internal investigation into that. I also understand that Mr. Gross is now fast-tracking a number of other initiatives to show progress on remedying these security breaches and, you know, normally this—we would take that as good news that you're giving priority and importance to trying to resolve this, but it appears that some of these initiatives Mr. Gross is spearheading are not the solutions that really are going to fix the problem but may exacerbate the problem and make it worse.

Mr. Gruenberg, are you aware that Mr. Gross has planned out—planned a rollout of a Digital Rights Management System?

Mr. GRUENBERG. Yes, Congressman.

Mr. LOUDERMILK. You are. Do you support that initiative?

Mr. GRUENBERG. As it's been explained to me, it seems like a reasonable step for us to take.

Mr. LOUDERMILK. Okay. And you trust that—is it Mr. Gross that has explained that to you?

Mr. GRUENBERG. Yes, sir.

Mr. LOUDERMILK. It has. Do you understand the benefit that DRM will have for cybersecurity protection at the FDIC?

Mr. GRUENBERG. I have some understanding. I don't hold myself out as a technology expert but I do have some understanding.

Mr. LOUDERMILK. Well, I spent 30 years in the IT business so I have somewhat of an understanding, but it is an evolving field. Basically, the Digital Right Management is a method of encrypting and applying rules of access or non-access to specific documents.

Mr. Gruenberg, I understand that the FDIC has this DLP that—and as I brought up the DLP earlier, you were nodding that yes, it did notify your data security team of that data being copied. Are you aware that the rollout of DRM will actually render DLP ineffective?

Mr. GRUENBERG. Not to my understanding, Congressman.

Mr. LOUDERMILK. So you haven't been briefed that it would actually render ineffective the current security system that actually notified you of that breach?

Mr. GRUENBERG. Not that I'm aware of, no, sir.

Mr. LOUDERMILK. Let me mention an email provided to the Committee by a whistleblower in the FDIC discussing the actual impact DRM will have. This email was sent on July 1, 2016, so it was pretty recent, and the subject line reads "risk to FDIC's data." Now, we have redacted the email and I am just going to summarize it, one, because we feel that if I read the details as it was written, it would provide—it would even exacerbate your current security risk that you have but also we have concerns of retribution on the whistleblowers within your organization. Basically this is from a senior expert within the FDIC that says, and I summarize or paraphrase, that there is a great risk of losing control over your data by simply releasing DRM without a lot of other work being done first, especially data classifications, labeling and access rights, which has not been done. It says each of these has to be done or essentially applying a DRM file will bypass the current DLP controls. This makes DRM a high risk to undetected data loss. It sounds like an environment that is supported by CIO, Mr. Gross, doesn't really understand what he's doing, and maybe he's just re-

sponding to the inquiries of this Committee to show that he's doing something but it will not actually have a positive effect but actually have a negative effect.

How do these types of fundamental security conflicts arise at the FDIC? Do you feel Mr. Gross has been giving you the full extent of what the system will do?

Mr. GRUENBERG. I do believe so, Congressman. I take very seriously the points you raise, and if I may, let us go back and take a look at the issue you raised, particularly in regard to DRM and its impact on the DLP. I think that's an important point. If we may, let us look into it and we'll come back to you.

Mr. LOUDERMILK. I appreciate it.

Now, I understand that right now there's no permanent Chief Information Security Officer in place. Is that true?

Mr. GRUENBERG. That is true. We're in the process of putting out a notice soliciting individuals for that position.

Mr. LOUDERMILK. Do you feel that position is very vital?

Mr. GRUENBERG. Central, sir.

Mr. LOUDERMILK. But yet you're going ahead with the rollout or fast-tracking rollout of a security program without this position being filled.

Mr. GRUENBERG. I think, if I may say, in regard to—if you're referencing DRM, I mean, that's still in the initial phase, so we will go back and consider the points you raised. This is going to be done in a very careful and deliberate way, and if the issues you raise are on point, we'll obviously take that into consideration.

Mr. LOUDERMILK. Well, I think it would be very advisable to do that, and I'm quickly—I've exceeded my time. But does the FDIC have any classified material of any quantity?

Mr. GRUENBERG. We do have a so-called SCIF.

Mr. LOUDERMILK. Is that information in danger if we continue to have conflicts like rolling out a DRM that will circumvent the current security protocols you have in place?

Mr. GRUENBERG. Not to my understanding but let me be sure I understand it before I give you a conclusive answer on that.

Mr. LOUDERMILK. My time's expired, and I now recognize the gentlewoman from Oregon, Ms. Bonamici, for five minutes.

Ms. BONAMICI. Thank you very much, Mr. Chairman, and thank you for calling this hearing.

Chairman Gruenberg, can you provide us with an update of the actions that the agency has taken to notify any individuals affected by all of the major data breaches? Have you offered credit monitoring services, for example? And if they have not been notified, when will that happen?

Mr. GRUENBERG. We are undertaking notifying and providing credit monitoring to all the individuals affected by those seven breaches.

Ms. BONAMICI. And Mr. Gibson, one of the two audit reports you released last week looked at a data-breach case in New York and suggested that the Insider Threat program could have potentially helped prevent that data breach. That language is pretty strong. The report mentions that the program was stalled in the fall of 2015. So will you please explain the importance of the Insider

Threat program, and what happened? Why did it stall? Because that's a pretty serious issue.

Mr. GIBSON. Sure. The Insider Threat program is an overarching program that allows the integration of information from multiple sources to assess whether an individual poses an insider risk to an enterprise. I think it's commonly accepted wisdom, and it's probably good wisdom, that the most significant threats that most organizations are going to face are insider threats, in other words, the risk of an employee or a person who's trusted within a computer network obtaining access or misusing access to data that's contained within or housed within a particular system. So we think that an Insider Threat program is an extremely important thing to do.

The program itself consists of a variety of different pieces, but beyond that, what's necessary is an overarching goal.

Ms. BONAMICI. I understand that, and I don't mean to interrupt——

Mr. GIBSON. That's——

Ms. BONAMICI. —but why did it stall in the fall?

Mr. GIBSON. That is unclear. I think that we've heard two different versions of the story as to why it stalled in the fall. From a senior management perspective, we've been told that there was concern that components of the program were conducting an investigation that was going too far and too fast with respect to an employee and that they needed to establish policies, procedures, standard operating procedures, and a means for managing the work that was being done before it continued.

We've heard kind of a different story at a different level of the organization where they believe that they were in essence directed to stop, and they got the message that there wasn't——

Ms. BONAMICI. I want to try to get another question in but I know that the Committee would appreciate follow-up on that when you determine exactly why that failed.

Mr. GIBSON. Okay.

Ms. BONAMICI. I wanted to follow up on Mr. Loudermilk's questioning, and I think this is best directed to you, Mr. Gibson.

The FDIC implemented a new version of its data loss prevention tool last September, and it was apparently the software that allowed you to identify the recent major data breaches but your office looked at the implementation of this tool, found some problems from September 2015 to the end of February 2016. The software identified 604,178 potential security violations and nearly 400,000 of those were related to removable media.

So it's my understanding that ultimately it was up to some individual to sort through those incidents and determine which are the most suspicious in order to see if they were legitimate downloads or indicated potential unauthorized activity, which seems a little bit like looking for a needle in a haystack.

So do you think that this DLP is a useful cybersecurity tool? What do you need to do to ensure it's used effectively? And just to follow up on Mr. Loudermilk's question, apparently now you're doing something that's inconsistent with that. And finally, since you've eliminated the removable media usage, has there been a re-

duction in the incidents that have been flagged by this DLP program?

Mr. GIBSON. Let me answer that as best I can. I think that the DLP tool as a tool is a tremendously important and helpful tool. I think that it requires a higher level of resources in order to be timely and effective. I would agree that digging through the volume of reports that the individual who's tasked with that has had to dig through really is a little like looking for a needle in a haystack, and I think that could be resolved, you know, by devoting some additional resources to it, and we've recommended that that be resourced differently. There may be other technical approaches that can be used as well. I wouldn't be the person to address that.

Ms. BONAMICI. By "additional resources," do you mean additional people looking for the needles in the haystack or do you mean some other approach?

Mr. GIBSON. Both.

Ms. BONAMICI. Mr. Gruenberg?

Mr. GRUENBERG. Congresswoman, if I can just add to that, I think a large percentage of the incidents being identified by the technology was a result of the use of removable media. So by discontinuing the use of removable media, we hope that's going to substantially reduce the number of incidents and allow for the more effective use of the technology.

Ms. BONAMICI. And you said you hope that it does, but do you know yet, have the—has there been a reduction in incidents flagged by the DLP program since the elimination of removable——

Mr. GRUENBERG. It's obviously a recent development. We can check into that and come back to you.

Ms. BONAMICI. Terrific. Thank you very much.

I yield back. Thank you, Mr. Chairman.

Mr. LOUDERMILK. The Chair now recognizes the gentleman from Texas, Mr. Neugebauer, for five minutes.

Mr. NEUGEBAUER. Thank you, Mr. Chairman.

Chairman Gruenberg, through the course of this Committee's transcribed interviews of FDIC employees, it is clear that CIO Larry Gross's fast-tracking a number of initiatives to show progress in remedying these cybersecurity breaches, and some of those have been mentioned. Normally, as the Chairman said, that would be welcome news, although it appears that some of these initiatives spearheaded by Mr. Gross are not the fixes needed.

Chairman Gruenberg, are you aware of Mr. Gross's initiative to replace all desktops at the FDIC with laptops?

Mr. GRUENBERG. Yes, Congressman.

Mr. NEUGEBAUER. And do you support that, and do you think that's a good idea?

Mr. GRUENBERG. As presented to me, it seems like a reasonable step to take. We're going to be implementing that in a careful and deliberate way. The use of laptops will enhance both the mobility and the continuity challenges that we face with our workforce. I think that's been part of the objective here.

Mr. NEUGEBAUER. Do you know what that's going to cost?

Mr. GRUENBERG. I can get that for you. You know, we provided laptops to our field employees in the previous year, and so this round is to provide it for our Washington employees.

Mr. NEUGEBAUER. So are you aware that a number of security experts at the FDIC strongly believe that replacing the desktops with laptops increases cybersecurity risk?

Mr. GRUENBERG. Look, I understand that there have been some statements to the Committee, and let me say, I'm sure those statements were made with good intent, and I appreciate the points raised. What we will do is, as for the points Congressman Loudermilk raised in regard to the DLP and DRM, is look into them, and, if we may, report back to you.

Mr. NEUGEBAUER. Well, just a little side note here. I think that the plan here has been to keep employees from taking data offsite, if I'm not mistaken, and if you start furnishing laptops with that information on there, it looks like to me we're moving in a different direction here, but——

Mr. GRUENBERG. Can I respond to that, Congressman?

Mr. NEUGEBAUER. Yes.

Mr. GRUENBERG. For what it's worth, and again, I want to be pretty cautious about representing myself in regard to technology, the laptops have value for both mobility and continuity of operations. If our operations are disrupted, there's value in our employees having that capability as well as tele-work. I think the belief is—and again, we'll review and come back to you on this—that a government-furnished equipment such as a laptop may be a more secure way to achieve that objective.

Mr. NEUGEBAUER. Well, I would suggest you look into that because I know a number of people are telling Mr. Gross that they don't think that's a good idea, and it appears that he's not listening, so I would encourage you to do your own due diligence.

Let me show you some testimony from former Acting Chief Information Officer and now Deputy CIO when asked about Larry Gross's laptop initiative. Put the slide up there.

[Slide.]

Question: "Are you—could you tell us a little bit more about the laptops. So under this new plan, would it replace the desktops that employees have at the agency?" The answer was, "It's not clear, and this is one of the things that has not been thought through. Some of the questions are, so is this—will this replace the desktop. So do you have both? So now I have a laptop and I have to take that back and forth. Now, again, I'm looking at it from a security perspective. Our focus has been security. What is the risk, you know? Why spend $5 million? Is this really going to help security posture for FDIC in terms of your spending something and you don't know what you're getting in return from the security perspective. There are many other things we can be doing to improve security posture at FDIC, and this is not at the top of the list, but this is what happens when decisions are made at the top level without including subject matter experts, folks from divisions, from business, and there's artificial deadlines imposed by this July 31st that are supposed to do all of this."

Mr. Gruenberg, there are other examples of similar testimony from IT and security experts at FDIC. I mean, I'm beginning to question Mr. Gross's proficiency in his job. Are these alarming to you?

Mr. GRUENBERG. Let me say, you raised—the points you raised, I think, are serious ones, and we'll take the opportunity if we may to review them and perhaps come back to you.

I would just say in regard to Mr. Gross, I think it's fair to say our Vice Chairman, Tom Hoenig's, perspective is one we believe Mr. Gross is a capable professional, and it's fair to say he assumed his position on November 2nd of last year so he's been on the job for 9 or 10 months. I think our sense is—and believe me, we will carefully consider the points you raised—but I think our sense is, we'd like to give him an opportunity to do the job and we'll evaluate that and I assure you we will hold him accountable, but we don't want to—we want to at least give him a fair chance to see-

Mr. NEUGEBAUER. Well, my parting comment is, as you know, and you and I both know, is that one of the things that your agency does is hold the financial institutions that you regulate under very high data security standards, and as you should because we're handling very sensitive information. I think it's extremely important that the FDIC set an example in that area, and I don't believe we're accomplishing that goal.

Mr. LOUDERMILK. I thank the gentleman, and Mr. Gruenberg, it sounds like the issue we're facing at FDIC is data getting out of the FDIC, and I would think that you would want to make it more difficult for employees to take data out, not make it easier with laptops. Maybe you should invest in a set of chains and locks instead of laptops.

At this point I recognize the gentleman from Illinois, Mr. Foster, for five minutes.

Mr. FOSTER. Thank you, Mr. Chairman, and thank you for everything that the FDIC does to make banking safer.

One of my favorite graphs in the universe is the number of bank failures as a function of calendar year from the Civil War to today where you see that banks back in the days of when it was the Wild West before the FDIC, you saw that hundreds of banks would fail in a typical year, and when the FDIC and related regulation came in, before we decided to dismantle it, we saw essentially zero bank failures and banks became a safe place. And so I want to thank you for everything that you've proven capable of.

Now, a couple of specific questions. The laptop thing, are these thin client laptops or are these full capability laptops with the data on drives and, you know, Bluetooth ports and all these sort of potential data leaks?

Mr. GRUENBERG. If I may, rather than answering that off the top, can I come back to you on that point?

Mr. FOSTER. Okay. Do you know in a general sense how your security compares to the security, say, at a large, sophisticated law firm or a large bank where they hold equally sensitive information. For example, do they allow employees to telecommute with sensitive data on laptops with what level of encryption, et cetera? As a very high-level question, could you sort of compare the fraction of your budget devoted to cybersecurity compared to, you know, what a large, sophisticated bank, for example, or large law firm would do? That would be a very useful comparison to find out whether you're underinvesting in this or whether it's just a problem that everyone is wrestling with.

Now, in relation to the removal of the portable storage devices there is an enormous data leak that everyone carries around in their pocket, and it's the very simple way of just taking pictures of screenshot. If you have access to read the clear text of a document, you can take a picture of it, and unless you plan to confiscate cell phones, it's very hard. There's a large class of insider attacks that you can imagine based on simply the existence of a cell phone in the employee's possession, and, that is the sort of thing they do. If you're talking about nuclear bomb designs, you cannot carry cell phones in. Is that the level of security that you plan on investing in or is there some intermediate level and you just live with the risks that are allowed that are intrinsic in that lower level?

Mr. GRUENBERG. You raise an important point. We've addressed the removable media issue. We're in the process of addressing paper production and controlling paper production as well. The issue you raised of snapping of a photograph of a screen and taking it with you is an issue we need to address but that's a significant challenge.

Mr. FOSTER. And a large number of secret ways of streaming the data out if you're allowed to download an executable on a laptop you own. There are many ways to communicate with similar programs on a cell phone that are going to be difficult to detect.

So I was just was wondering if you see the endpoint here to be the endpoint comparable to nuclear security or comparable to best practices at a big bank.

Mr. GRUENBERG. That's a—you know, I don't know—I would like to think we would at a minimum achieve best practices for both government agencies and the private sector. I think that would be a reasonable objective for us.

Mr. FOSTER. And are you looking at the tradeoff between just cloud-based everything and just thin clients with no real data storage locally, which is in some people's view the best practice endpoint for this, versus the dangers of even having employees with encrypted data that they sometimes can forget to encrypt on their laptops and carry home and lose the laptop and that sort of fun class of data breach.

Mr. GRUENBERG. That's also a set of issues we have under review.

Mr. FOSTER. Okay. Are there conferences where all the federal agencies and the best and brightest in industry get together and identify the best practices in this pretty terrifying environment?

Mr. GRUENBERG. There has been an enormous amount of interaction first among the federal agencies related to cybersecurity and expanded efforts for interaction with industry. I think there's an understanding that there needs to be a level of collaboration between the public and private sectors to begin to get arms around the cyber issue, and there are committees that have been established both made up of the federal agencies and made up of industry that also interact together in terms of trying to increase cooperation.

Mr. FOSTER. So you're not really going off in a corner and inventing something new? You're collaborating with what is really a government-wide—at least government-wide if not industry-wide?

Mr. GRUENBERG. I think that's fair to say.

Mr. FOSTER. Okay. Let's see. One last thing if I may, one last question. Can you contrast your level of security compared to the very, very large number of state banking regulators? Would you hazard a guess as to whether there're likely state bank regulators out there that have comparable vulnerabilities?

Mr. GRUENBERG. Well, it's a fair question. I'm not sure I'm in a position to comment on it.

Mr. FOSTER. Okay.

Mr. GRUENBERG. I would say as a general matter, it wouldn't surprise me if our level of investment were greater given the resources, but you'd really have to look into it.

Mr. FOSTER. All right. Thank you.

Yield back.

Mr. LOUDERMILK. The Chair recognizes the gentleman from Oklahoma, Mr. Bridenstine.

Mr. BRIDENSTINE. Thank you, Mr. Chairman.

Mr. Gruenberg, you have said that the FDIC takes seriously its commitment to improving its cybersecurity posture. Is that correct?

Mr. GRUENBERG. Yes, sir.

Mr. BRIDENSTINE. And you have said that improving the cybersecurity posture of the FDIC is one of your highest priorities. Is that correct?

Mr. GRUENBERG. Yes, sir.

Mr. BRIDENSTINE. So why is it that you don't do strategic IT planning?

Mr. GRUENBERG. Well, it's my understanding that under the CIO's direction that that is done, but let me check on that to be sure that's an accurate answer.

Mr. BRIDENSTINE. Mr. Gibson, do you agree that strategic IT planning is done at FDIC?

Mr. GIBSON. Sir, I've never really looked at that question. If you could help me out a little bit, what exactly do you mean by "strategic IT planning"?

Mr. BRIDENSTINE. Well, the idea that we're not reactionary but instead we're planning ahead of time and not just reacting to every individual incidence.

Mr. GIBSON. Well, one of the subjects that we intend to look at in the very near future is the whole question of enterprise architecture. Enterprise architecture basically is understanding the design of the FDIC's network and its overall IT system and its IT structure. We've commented for years that we thought that more resources or effort needed to be placed in the enterprise architecture area. We intend to look at it specifically now because we do place great value on that in terms of being able to direct the resources and investment that are being made and understand better the networking and the security components of the environment that we're looking at. To the extent that that helps answer the question, it's something that we'll be looking at very specifically in the near future.

Mr. BRIDENSTINE. That's perfect.

And Mr. Gruenberg, will you commit to evaluating the entire IT enterprise architecture and moving forward with strategic IT planning?

Mr. GRUENBERG. Yes, Congressman, I think that's an excellent suggestion. Thank you.

Mr. BRIDENSTINE. Okay. Mr. Chairman, I yield back.

Mr. LOUDERMILK. The Chair recognizes the gentleman from Colorado, Mr. Perlmutter, for five minutes.

Mr. PERLMUTTER. Thanks, Mr. Chair.

So my first question to you two is, how does Bell's theorem or the Drake theory apply to the breach? Oops, that was for the astrophysicist from a couple days ago. I apologize for that.

All right. I'll stop messing around.

Mr. GRUENBERG. I was looking over at Fred——

Mr. PERLMUTTER. I'll stop messing around.

First, like Mr. Foster, I want to thank both of you for the job that the FDIC does. We came through a very difficult time, 2008, 2009 and 2010, expected a lot—I expected more failures, a lot of work between the insurance corporation and the banks to stabilize them and grow the economy. So the big picture, thank you very much.

All right. So now I'm just going to go back to sort of how I can understand this, and there's been somebody who's a thief, he's robbed you, and then the question is, what was taken, and who and how many people have been robbed or otherwise hurt, and then what are you going to do about it. So I assume in these different instances, somebody—the robber, the thief is facing some criminal liability of some sort or another. Am I wrong?

Mr. GIBSON. Sir, we have a number of investigations that are currently open with regard to a number of the matters that we're talking about here today. I don't know what the ultimate outcome of those will be but the goal was to determine whether there is criminal responsibility that can be imposed on anybody, and if there is, we'll pursue it with our partners in the Department of Justice.

Mr. PERLMUTTER. If I went back to my law firm and one of my partners or one of the staff took a file how would I respond? I'd say give it back but the problem you all face is that when somebody takes a file, they take a million files, and I think that's the purpose of today's panel, to try to understand how far and wide these things are, and how you're building your defenses to that disgruntled employee or somebody who made a mistake and bang, it's all out there.

So you know, some of the questions, Mr. Chairman, have been directed to you about reprimands within the organization to the guy who just took over and is trying to figure out where the vulnerabilities are and who were the thieves I don't understand why reprimanding him at this point makes any sense. But I do understand the Committee's concern that if the FDIC is somehow robbed, that one, we need to check your defenses, but two, somebody's going to pay for it, you know, Edward Snowden, so it isn't like you're all by yourselves getting robbed. I mean, the NSA, the CIA, the Office of Personnel, Anthem Blue Cross, Target, Chase, you name it, everybody's been hacked. But you are the backstop for banks. So what are you doing to try to build up your defenses?

Mr. GRUENBERG. Well, Congressman, in this set of incidences, for all of these breaches, just from a technology standpoint, the underlying vulnerability, as I indicated, was allowing the use of so-called

removable media—flash drives, thumb drives—which allowed an individual to download sensitive information on to a device like this and basically walk off with it.

Mr. PERLMUTTER. All right.

Mr. GRUENBERG. That was the—and we've now, it's fair to say, discontinued the use of those devices.

Mr. PERLMUTTER. Let me ask you this. The three of us are lawyers, all right? So how is it—I understand the investigations are proceeding, but if somebody takes off with a thumb drive, has any of this been put to nefarious use? Because if it has, then that guy should be under indictment or in jail. What really is happening there?

Mr. GRUENBERG. On the criminal side, I really should leave it to the IG because that's the IG's responsibility. I think in—well, Fred, do you——

Mr. GIBSON. So I guess the best way that I can answer that question is to say that we are pursuing cases where we believe that there is a basis for bringing them and we're just not at a point yet where we can disclose publicly exactly what the status of that case is, but yes, we are pursuing investigations in the specific areas you're concerned about.

Mr. PERLMUTTER. All right, well thank you, gentlemen. Thank you for your service to the country, and I yield back.

Mr. LOUDERMILK. The Chair recognizes the gentleman from Alabama, Mr. Palmer.

Mr. PALMER. Thank you, Mr. Chairman. I have a slide, if we could get that slide up, please?

[Slide.]

Very good. Thank you.

I want to walk through this with you. I'm going to read this transcript. You can read it if you can see it well enough on the slide. This was between FDIC personnel in regard to the breach, and it says, "Just to be clear here for the record, there was a penetration of the FDIC network system generally by an outside party that was malicious, right? Correct?" and the answer was, "Yes." And the FBI alerted the FDIC, the appropriate people within the FDIC, that this was the case, and one of the potential fixes or appropriate actions was to shut down or turn off the entire FDIC system to eradicate the intruder, and the answer was yes, that was recommended. Okay, now after that, it was—the FDIC employee said, "Now, after that, it was kept—I'm out of the loop except for Ned came into my office to tell me that this incident that Russ Pittman said: This can't get out here, this breach information. We can't do anything to jeopardized"—that's their word—"the chairman getting, when they vote, getting approved for because it's"—and the questioner, "A Senate-approved position? Confirmed." "Yes." You can take down the slide.

Mr. Gruenberg, are you aware that the FDIC employee attempted to cover up the fact that a foreign nation hacked into FDIC systems in an effort not to jeopardize your confirmation as chairman by the U.S. Senate?

Mr. GRUENBERG. No, sir.

Mr. PALMER. You are not aware of that?

Mr. GRUENBERG. No, sir.

Mr. PALMER. You've never been made aware of it?
Mr. GRUENBERG. Never, sir.
Mr. PALMER. Are you concerned that the——
Mr. GRUENBERG. There was a report that came out yesterday. That was the first that I had been made aware.
Mr. PALMER. So no one within the FDIC discussed this with you even before the hearing that this might come? The first time you saw it was yesterday in the media?
Mr. GRUENBERG. Yes, and when that—the committee interim report was released and there was a reference to it. That was the first I became aware of it.
Mr. PALMER. So you testified that you've never—you did not hear that before yesterday?
Mr. GRUENBERG. No, sir.
Mr. PALMER. Okay. Are you concerned that the FDIC officials attempted to shield details of the incident from knowledge of the individuals outside the FDIC including the Inspector General until after your confirmation? Does that concern you?
Mr. GRUENBERG. I understand this was represented. I can't speak to the accuracy——
Mr. PALMER. We can give you a copy of the transcript.
Mr. GRUENBERG. I understand, but, you know, it—I can't speak to the accuracy. If it was accurate, certainly.
Mr. PALMER. When did you first learn that the breach occurred?
Mr. GRUENBERG. Well, this goes back to an incident in 2010 and 2011, I believe.
Mr. PALMER. Were you aware of it then?
Mr. GRUENBERG. I was made aware of it, I believe, for the first time in 2011, and as you may be aware, our Inspector General—undertook an investigation of this and issued a report in 2013. I believe the finding of the report as I indicated in my opening statement, is that in regard to this incident, both myself and other members of the Board and senior executives were not fully informed.
Mr. PALMER. I've got a couple other questions. Are you confident that the FDIC's current cybersecurity posture can prevent a similar breach from occurring? It's a yes or no.
Mr. GRUENBERG. If I may, as the—I think we are improving our systems. I think—I want to say in light of OIG reports—I think it's fair to say we are working hard to address the issues identified. So I don't want to——
Mr. PALMER. So you're not totally certain that it's secure?
Mr. GRUENBERG. I think——
Mr. PALMER. Let me ask you this——
Mr. GRUENBERG. Congressman——
Mr. PALMER. —in the context of how these breaches occurred, if I may, does the—where the employees taking information on their way out after they've left employment, does the FDIC have an employee handbook manual?
Mr. GRUENBERG. I would have to check but I believe—I assume we have something like that.
Mr. PALMER. Based on that answer, I would assume you haven't read it.
Mr. GRUENBERG. I can't say I've looked at it, sir.

Mr. PALMER. I think it might be a good idea if you became familiar with it and make sure that you have a policy in there that is clear that it is prohibited for any employee upon leaving their employment that they cannot take any information with them, and I think if that had been clearer, that might not have happened. It may have happened anyway, particularly with a disgruntled employee.

Mr. GRUENBERG. Congressman, if I may say, I do believe there is such a requirement so that when an employee leaves the agency, they have to sign a statement to that effect.

Mr. PALMER. They do?

Mr. GRUENBERG. Yes.

Mr. PALMER. Well, were these people prosecuted? Because that's a prosecutable offense.

Mr. GRUENBERG. That's what the IG is looking into, I believe.

Mr. PALMER. Okay. Let me say this, Mr. Chairman, and I'll wrap it up.

I find it interesting that some at the FDIC apparently thought your confirmation as Chairman was more important than taking immediate action to protect almost 31,000 banks and 160,000 individuals, as it turns out the total here. It's as though these banks and their depositors and customers were acceptable losses, collateral damage, to ensure that you would—there would be no obstacles to your confirmation. That concerns me. That is indicative of some political calculations within the FDIC that in my opinion were totally inappropriate. I yield back.

Mr. LOUDERMILK. I thank the gentleman.

Mr. Gruenberg, as you're aware, this hearing is about security breaches, cybersecurity breaches, and your efforts to mitigate future breaches, but I'm growing more concerned of the lack of preparation because quite often, many times in most every witness, you've said let me get back to you on that, and in one case, what really concerns me, you said you may get back to us with that——

Mr. GRUENBERG. I'll get back on every point, sir. I didn't mean to——

Mr. LOUDERMILK. Oh, okay. That helps a little bit. But also getting a little more concerned, we don't expect you to know the answer to every intricacy in there but not knowing whether you even have a policy handbook is concerning, and a lack of staff here as advisors with you is—may lead some to believe that maybe you weren't as prepared or take this as seriously as we think you should.

With that, I recognize the gentleman from Virginia, Mr. Beyer, for five minutes.

Mr. BEYER. Thank you, Mr. Chairman.

I believe we can all agree that the FDIC has suffered from some serious data breaches and that some of their responses to the Committee were initially not complete and that the original analysis of these major data breaches by senior FDIC officials was not adequate or fully accurate. However, I don't agree that we can or should infer from the facts that the Committee has gathered to date as the Majority has clearly done that individual FDIC employees intentionally lied to this Committee or have engaged in deliberate obstruction of this Committee's investigation.

Unfortunately, the Majority appears to have selectively pulled some information that helps them paint that narrative. They ignore some records and have intentionally not interviewed certain witnesses who may have presented a fuller understanding of the agency's actions that the Majority has called into question.

As one key example, the Majority staff report refers to one FDIC official who the report stated, "deliberately tried to prevent FDIC attorneys from creating records that would be responsive to the Committee's request in this investigation."

But the initial request not to create emails regarding certain investigations of the agency's investigation was documented in an email from one FDIC employee on October 29, 2015, which was long before the Science, Space, and Technology Committee began an investigation, long before we were even aware of the breach.

So while this email raises legitimate questions about why FDIC employees were directed not to put certain information in emails—that's certainly inexcusable—it occurred one day before the OMB memo 1603 was issued and 4 months before the Committee even became aware of the data breach at the FDIC. So to suggest this direction was part of an effort to obstruct the Committee's investigation makes no sense, is frankly misleading when you examine all the records the Committee has obtained.

So I'd like to seek unanimous consent to enter this email of October 29, 2015, into the record.

Mr. LOUDERMILK. Without objection, so ordered.

[The information appears in Appendix II]

Mr. BEYER. Thank you, Mr. Chairman, and Mr. Chairman Gruenberg, I read carefully—I listened to you but I also read the 15-page statement that you submitted for the record, and I just wanted to thank you for not the disasters before but for taking full responsibility, for trying to be as clear and transparent as possible, for coming together with a comprehensive plan which takes up most of that 15 pages, and near as I can tell, fulfilling all of the Inspector General's recommendations. I thought Chairman Smith's opening question, which is to the Inspector General, are you as the leader of the FDIC doing everything that they recommended, and let me, Inspector General, ask you that one more time to make sure that we're all on the same page.

Mr. GIBSON. Sir, they gave us a series of responses to our recommendations that we consider to be responsive. What we'll be doing is, we'll be following up to monitor the implementation of the things that the FDIC has indicated they will do and to determine whether they've been effective.

Mr. BEYER. Great, great. We would only expect that you would continue to make sure that the chairman and his team follows through on the recommendations you've made.

Mr. Chairman, in the back and forth with my good friend from Alabama, where you were taking some heat about the employees who were shielding you through the nomination process, were you aware that they were shielding you, and did you take any personnel action once you became aware?

Mr. GRUENBERG. I certainly was unaware, Congressman, as I indicated. I learned about it for the first time yesterday, and I just would be cautious. I understand it was asserted by an individual

in an interview, but there hasn't been a review of what actually occurred here, so I'd be cautious, you know, about the accuracy of the representation.

Mr. BEYER. Okay. Good. Thanks. But you certainly would agree that this is inappropriate?

Mr. GRUENBERG. Oh, no question, if indeed it's true.

Mr. BEYER. Yeah. Thanks. Much has been made about the seven people that took the records out, the excess of 10,000 per person. What is the long-term follow-up plan to make sure that the data breaches have no ongoing effort? You know, sometimes the records are stolen by whomever, and it could be 2, 3, four years before they try to apply for a credit card or a car loan or something like that.

Mr. GRUENBERG. Well, as a threshold, I think we're addressing the technological vulnerability related to the removable media that sort of underlay each of these incidences, so hopefully as a threshold, that'll be helpful in addressing it. We'll also be implementing policies and procedures to carefully monitor any activity and have a very strong system of controls relating to any employee who may be separating from the agency.

Mr. BEYER. But I'm specifically concerned about the records that were already out there, not breaches still to happen but breaches that already did occur.

Mr. GRUENBERG. Yeah. For the ones that have been identified, and we have recovered the devices, we can't say with certainty that there was no dissemination. I don't know that we can ever demonstrate that conclusively. At least thus far, we haven't had evidence of dissemination.

Mr. BEYER. Okay. Great. Thank you, Mr. Chairman.

Mr. Chairman, I yield back.

Mr. LOUDERMILK. I thank the gentleman from Virginia, and Mr. Gruenberg, since you are going to get back with us on some things, would you please provide this Committee the copy of the handbook that was mentioned earlier?

Mr. GRUENBERG. Yes.

Mr. LOUDERMILK. Also, notice to the members of the Committee, we do intend on doing another round of questioning for those—this is an important matter. We'll make sure everyone gets their ample opportunity to ask their questions.

With that, I recognize the gentleman from Louisiana, Mr. Abraham, for five minutes.

Mr. ABRAHAM. Thank you, Mr. Chairman.

Mr. Gruenberg, when did you first become aware of the Florida incident where 10,000 people's records were compromised? When did you become aware?

Mr. GRUENBERG. I think I was informed in— the incident occurred on October 15th. It was identified on October 23rd. I believe I was notified for the first time in November, I think November 19th.

Mr. ABRAHAM. So about a month?

Mr. GRUENBERG. Yes, sir.

Mr. ABRAHAM. What was your role in deciding whether to report that to Congress or not?

Mr. GRUENBERG. I didn't. As the IG noted in its report, I didn't have a role in that.

Mr. ABRAHAM. So I mean, you couldn't have been proactive? Or could you have been proactive in reporting that to Congress if you so chose?

Mr. GRUENBERG. It was a judgment made by our CIO working with the data breach management team——

Mr. ABRAHAM. And that was the gentleman that took the hand on November 2nd?

Mr. GRUENBERG. Yes, sir.

Mr. ABRAHAM. And I understand that he was new to the job and he has been in the job eight or nine months and that he's learning the job but, you know, I might suggest this is not an on-the-job training job. He should have come very well vetted and prepared to do the job on day one. So it does concern me that, you know, we're taking this type of attitude—well, he's learning the job, so to speak, and you know, we hate it that he was thrown into the fire that early. I mean, if he would have been thrown into the fire the day he got on the job, he should have been able to do the job.

Mr. GRUENBERG. It's a fair point, Congressman. He came, as you can—if you reviewed his bio—with considerable experience in this area. I was referring to his learning a new agency.

Mr. ABRAHAM. Well, I understand that, but again, these are questions you ask in a pre-employment brief, and he knew the job before he took the job.

Did you ever resist the OIG's suggestion to report the Florida incident as a major incident to Congress?

Mr. GRUENBERG. No, Congressman.

Mr. ABRAHAM. Okay. Mr. Chairman, I yield back.

Mr. LOUDERMILK. The Chair recognizes the gentleman from Ohio, Mr. Davidson, for five minutes.

Mr. DAVIDSON. Thank you, Mr. Chairman. Thank you both for coming here, and I appreciate the work that you do. The FDIC does have a nice track record of success in securing our financial institutions. I'm very concerned about the recent record of securing our data which is at stake, so thank you for taking that seriously.

And one of the questions I've got going back to this Florida incident, Mr. Gibson, did your staff find that the FDIC's representations of the Florida breach were inadvertent, non-malicious, and the breacher was cooperative? Did you find those as accurate statements?

Mr. GIBSON. No, sir, we wouldn't agree with that.

Mr. DAVIDSON. Mr. Gruenberg, why would your staff provide that information during the Committee's briefing to Congress that they were simply trying to understand how it actually occurred?

Mr. GRUENBERG. Congressman, I believe—and I understand the IG's perspective on this. I think the assessment made rightly or wrongly by our CIO in conjunction with other staff in the Legal Division was that it was inadvertent. It may have been a misjudgment but that was the judgment—the conclusion that was reached.

Mr. DAVIDSON. And just to restate it, I think it's been covered, but to be very clear, the individual at the center of this was not cooperative and was—since it was not inadvertent. It was therefore advertent. It was non-malicious, therefore, it was malicious. Has there been any action taken against this individual?

Mr. GRUENBERG. Well——

Mr. GIBSON. Sir, she's a former employee, so from the FDIC's perspective, I assume there really isn't any action that they're able to take, and again, all I can say with respect to our ongoing work is that there are a number of matters that we're looking at that haven't reached the stage where we can discuss it publicly.

Mr. DAVIDSON. You don't feel that there's a crime that has been committed here?

Mr. GIBSON. Sir, whether I feel there's a crime or not probably isn't the issue. The question is whether an individual was engaged in behavior that the Department of Justice would agree constitutes a crime and they can bring an indictment against someone.

Mr. DAVIDSON. We've seen that seems to be a pretty high bar lately.

What would happen—you guys cover our banks and our financial institutions, and really audit many of these same transactions. So what would happen if a financial institution had a similar data breach?

Mr. GRUENBERG. I asked that question, Congressman. I think—a couple of things. They would have to identify the harm or risk of harm, they would have to notify customers that are impacted if there is a risk of harm, and there would be an expectation that they would notify their regulator.

Mr. DAVIDSON. And they would be very clear under Dodd-Frank in particular that they would notify you, correct?

Mr. GRUENBERG. I believe it's actually under the Graham-Leach-Bliley Act that there was a provision relating to this.

Mr. DAVIDSON. Right. And how would—how would you react if a financial institution provided patently false information to you during your investigation? What sort of course of action would you have in following up with that institution?

Mr. GRUENBERG. I think the procedure would be that there would be a follow-up at the next examination. We would review the handling of the case. We would review their systems, to see whether there was, you know, a failure. If there was evidence of intentionality in terms of not reporting that, that would be an additional matter we'd have to take into consideration.

Mr. DAVIDSON. What sort of signs would you look for to say that they were actually taking the matter seriously? Would you consider it serious if they kept all the same personnel and practices in place?

Mr. GRUENBERG. I think the threshold—and again, I'm not an examiner, but I'll just try to respond—I think would be what systems do they have in place and the effectiveness of those systems to deal with these kinds of issues.

Mr. DAVIDSON. Here's the concern I've got coming into the meeting, and frankly, only made worse during the conversations, is that we're focusing on one or two individuals, and really, the IT department at your agency can't be as strong as one new employee. You've got a robust staff, and so I'd be curious to know what sort of recommendations and dialog and, frankly, from the whistleblower information, it seems like there's really not a lot of support for some of the direction your new CIO is going. And that doesn't mean that there's—that it's accurate, to your point. I appreciate your desire to look into it. But I'd also ask you to look into the cul-

ture because, frankly, it sounds like this culture is perhaps maybe partisan cover-ups and maybe just concern that it's impossible to fail. There's a lot of pressure to perform, and so there's cover-ups there, and so a culture that doesn't provide the kind of transparency is not likely to be able to deliver the kind of results that your mission requires, and so I'm very concerned about that.

Thank you. I yield back, Mr. Chairman.

Mr. LOUDERMILK. The Chair recognizes the gentleman from Illinois, Mr. LaHood, for five minutes.

Mr. LAHOOD. Thank you, Mr. Chairman, and I want to thank both of you for being here today. I appreciate it very much.

I guess I want to just focus a little bit on some of the transcript interviews that have been conducted with FDIC employees seem to indicate that there has been a concerted effort by the legal department at FDIC on instructing employees on how to respond when it comes to cybersecurity breaches as it relates to emails, and it seems like a real effort, Mr. Gruenberg, to limit the exposure to Congressional and FOIA requests, and that's really concerning to the Committee and to us because what that leads us to believe, or me to believe, is that you're hiding facts or circumstances surrounding these breaches, and particularly when it comes from the legal department because that's who your employees rely upon in your department, and I guess just from a foundational standpoint in looking at these very serious cybersecurity breaches, Mr. Gruenberg, do you take transparency seriously at the department?

Mr. GRUENBERG. Yes, Congressman.

Mr. LAHOOD. And are you committed to working with this Committee and the Inspector General to prevent breaches in the future?

Mr. GRUENBERG. Yes, very much so.

Mr. LAHOOD. And as Chairman of the FDIC, you speak on behalf of the Agency. Is that correct?

Mr. GRUENBERG. Yes, but just acknowledging I have a board that I have to consult and work with as well.

Mr. LAHOOD. And can you—I want to get into a couple of these interviews that were done. Can you give us—you're a lawyer, correct?

Mr. GRUENBERG. Yes, sir.

Mr. LAHOOD. And in fact, you served as Senior Counsel to the Senate Banking Committee, correct?

Mr. GRUENBERG. Yes, sir.

Mr. LAHOOD. So the legal department instructing FDIC employees not to discuss matters related to cybersecurity and breaches, why was that being done?

Mr. GRUENBERG. I understand that was represented in the report. If I may, let us look into it and come back to you on it.

Mr. LAHOOD. Well, that's hard to take that answer when your legal department is giving that advice.

I want to direct your attention to a specific transcript. It's up on the screen there. This is an excerpt for—these are questions that were asked, and the nice thing about transcripts is, it gives us the questions and the answers that were given. "Are you aware of any instructions given by anyone at the FDIC to not discuss certain subject matters in an email?" That's the question. Answer: "Yes."

Question: "Could you shed a little light on that?" That's the question. Answer: "I received the same instructions directly from Roberta McInerney, and Roberta McInerney's instructions to me were, quote, ″Do not discuss deliberations over the applicability or implications of OMB 1603 in an email.″" Question: "You mentioned that instructions from Roberta McInerney gave to you. Was that directly to you?" Answer: "Yes. Roberta McInerney gave those instructions directly to me."

So I look at that from employees, and that seems to be a pattern here. Were you aware that she was giving those instructions to FDIC employees?

Mr. GRUENBERG. No, I wasn't, Congressman.

Mr. LAHOOD. When you found out she was doing that, what did you do?

Mr. GRUENBERG. This was represented, I gather, in an interview by one of our employees with the Committee, and so it is now something that we will——

Mr. LAHOOD. When did you become aware of it?

Mr. GRUENBERG. I know it was contained in the report that was released yesterday. There may have been emails that we provided, so I'd have to check specifically, but that's something we will have to——

Mr. LAHOOD. When did you become aware that she was doing this?

Mr. GRUENBERG. I can't tell you specifically. I'd have to go back and check the record.

Mr. LAHOOD. Would you—I mean, just can you give us a time frame? Would it have been two months ago, a month ago?

Mr. GRUENBERG. It would have been—I really have to check but it would have been—I'd have to look at the production that we made to the Committee when we——

Mr. LAHOOD. I'm asking for a time frame when you became aware that she was instructing employees to do this.

Mr. GRUENBERG. I would assume in the last few weeks but I'd have to check on it.

Mr. LAHOOD. When you found that out, what did you do?

Mr. GRUENBERG. We haven't taken any action on it yet, sir.

Mr. LAHOOD. So when you found out, you have not done anything?

Mr. GRUENBERG. Not thus far.

Mr. LAHOOD. Were you complicit in those instructions?

Mr. GRUENBERG. No, sir.

Mr. LAHOOD. Did you ever advise employees in your department to do what Roberta McInerney did?

Mr. GRUENBERG. No, sir.

Mr. LAHOOD. Does every employee at the FDIC take an oath of office?

Mr. GRUENBERG. I believe so.

Mr. LAHOOD. I want to put up on the screen there the oath. I believe this is the oath that's taken by employees. I believe you took this oath and everybody else there. You're familiar with that, correct?

Mr. GRUENBERG. Yes, sir.

Mr. LAHOOD. And do you believe that your employees are abiding by that oath of office?

Mr. GRUENBERG. I believe so.

Mr. LAHOOD. And can you certify to the Committee that all your employees are abiding by this oath?

Mr. GRUENBERG. I don't know that I have the capacity to do that.

Mr. LAHOOD. Thank you. Those are all my questions, Mr. Chairman.

Mr. LOUDERMILK. I thank the gentleman from Illinois, and I also may add that the questions by Mr. LaHood is corroborated by the email that was entered into the official record by Mr. Beyer that this was indeed happening, so I thank the gentleman from Virginia for that.

I now recognize the gentleman from Texas, Mr. Weber, for five minutes.

Mr. WEBER. Thank you, Mr. Chairman. That was an interesting discussion between you and Mr. LaHood, Mr. Gruenberg. I might give you some unsolicited advice. You can actually download the manual onto a thumb drive and walk out with it probably as some other things too if you want.

Did you become aware of that information before the report was released, you talked about yesterday, you said a few weeks?

Mr. GRUENBERG. I'd really need to check just to be sure I give you accurate information.

Mr. WEBER. Well, that's very, very interesting.

You have—you said earlier in a discussion with Randy Neugebauer in an exchange that you were careful about representing yourself as being with technology or something to that effect. So who would—you're aware that the Insider Threat program is aimed at identifying potential employees. Since you're not a technology person, who advises you on that program?

Mr. GRUENBERG. The—we have both the CIO and our Division of Administration is responsible.

Mr. WEBER. Okay. Is that program contained in the manual? You probably don't know because you haven't read the manual.

Mr. GRUENBERG. No, that's—I don't believe—it's a program we're in the process of establishing.

Mr. WEBER. So it was established at one point but you halted it?

Mr. GRUENBERG. No, it was in the process of being developed.

Mr. WEBER. So it was being developed and you halted the development?

Mr. GRUENBERG. Well, I believe the term used in the IG's report was "stall." I think there was a process of developing the program over a period of time. My understanding of what occurred is that there was a lack of follow-through in bringing it to completion.

Mr. WEBER. Who advises you on that program's progress or lack thereof?

Mr. GRUENBERG. It would be, I think, both our Division of Administration and our CIO.

Mr. WEBER. Can you give us the name?

Mr. GRUENBERG. I can get those for you, sure.

Mr. WEBER. So you didn't have any discussion with individuals that you know the name of that said look, the program needs to be halted?

Mr. GRUENBERG. Oh, no, no. I think there's—no, sir.

Mr. WEBER. So you just halted it on your own without conferring with anybody?

Mr. GRUENBERG. No, as I indicated, my understanding is that the program was in development and it was not brought to completion in a timely way.

Mr. WEBER. So who halted that program?

Mr. GRUENBERG. As I said, I don't know that it was halted. I think the term used in the IG's report——

Mr. WEBER. Okay. So who—it quit being developed. Now we're parsing words.

Mr. GRUENBERG. I think it never stopped being developed. I think it slowed down. It wasn't brought to fruition in a timely way.

Mr. WEBER. But nobody advises you on this program?

Mr. GRUENBERG. I think both the Division of Administration and the CIO——

Mr. WEBER. But you'd have to have one person who was an IT expert, right, that actually knew that program inside and out and could come report to you?

Mr. GRUENBERG. We have a security group in our Division of Administration that I think is the lead on that.

Mr. WEBER. Who do they report to?

Mr. GRUENBERG. They would report to the Director of the Division.

Mr. WEBER. And who would that Director of that Division report to?

Mr. GRUENBERG. The Director reports to our Chief Financial Officer.

Mr. WEBER. And who would that Chief Financial Officer report to?

Mr. GRUENBERG. To me.

Mr. WEBER. To you. And you had no communication up that line to talk about that program and it needed to be stopped being developed or halted or whatever parsed word we want to use?

Mr. GRUENBERG. No, sir.

Mr. WEBER. No communication whatsoever?

Mr. GRUENBERG. No, I was briefed on the program, and it was an understanding that we wanted to develop it in a careful way.

Mr. WEBER. And you were briefed by who?

Mr. GRUENBERG. By the individuals I mentioned.

Mr. WEBER. And the names?

Mr. GRUENBERG. The Director of our Division of—I'd have to—I should check, you know, who participated in the briefing to be sure I——

Mr. WEBER. But you did name two, Director of the Division and the CFO, I think.

Mr. GRUENBERG. Yeah, I would want to just check for accuracy as to who took part in the briefing just to be sure.

Mr. WEBER. So you're not sure that either one of those people briefed you?

Mr. GRUENBERG. I believe they did. I just want to check the record to be sure I'm giving you accurate information.

Mr. WEBER. Okay. And you can get back to us in writing with that?

Mr. GRUENBERG. Certainly.

Mr. WEBER. Mr. Gibson, do you understand the Insider Threat—maybe you could brief Mr. Gruenberg. Do you understand the Insider Threat program?

Mr. GIBSON. I try to.

Mr. WEBER. Okay.

Mr. GIBSON. Do I understand it? Yeah, I mean, the basic purpose of the program——

Mr. WEBER. Do you know why it was halted last fall, or not—"halt" is not the right word—no longer developed?

Mr. GIBSON. We had a discussion about that a little earlier in the hearing today, and, you know, basically we've heard two reasons for that. You know, management believed that the program was moving too far, too fast, too quickly, that it needed to, you know, develop some standard operating procedures and processes and so forth. The people who were a lower level of the organization believed that they were essentially told stop, and——

Mr. WEBER. Is there communication about that? When you said they believed they were told to stop, was there communication about that we can get?

Mr. GIBSON. There were a couple of briefings, as I recall.

Mr. WEBER. Any emails?

Mr. GIBSON. None that I'm aware of, sir.

Mr. WEBER. Okay. Would you recommend that it be unhalted or un—whatever the term you want to use?

Mr. GIBSON. I think the most significant recommendation in one of the audits that we've completed is that the FDIC establish a formal Insider Threat program.

Mr. WEBER. Okay. Chairman, did you say there's going to be a second round of questioning?

Mr. LOUDERMILK. Yes, we will, until we get through everyone or votes are called, which we anticipate is going to be about 40 to 45 minutes.

Mr. WEBER. Well, then I'll go ahead and yield back. Thank you.

Mr. LOUDERMILK. The Chair recognizes the gentleman from Illinois, Mr. Hultgren, for five minutes.

Mr. HULTGREN. Thank you, Mr. Chairman. Thank you both for being here.

Mr. Gibson, I want to commend your good work on these audit reports. Your team has done an outstanding job.

Mr. GIBSON. Thank you, sir.

Mr. HULTGREN. I want to point out, however, that the FDIC has been without a Senate-confirmed Inspector General for over a thousand days. Since September 2013, there's only been an Acting Inspector General. Congress, the House in particular, relies on the IGs to be independent watchdogs. To a certain extent, they are our eyes and ears within the department or agency.

Mr. Gibson, would having a Senate-confirmed IG empower your office, and if so, how so?

Mr. GIBSON. Sir, I think under the IG Act, the idea of a Senate-confirmed IG is to create a position with significant independence within the agency and the ability to handle things in a totally independent manner. I mean, all I can say is, we've done our best to

preserve our independence through this period of time, and I believe we have.

Mr. HULTGREN. I appreciate that.

The Committee has learned that the Agency has access to your Office of Inspector General emails in some cases as well as emails between your office and the informants you may have within the agency. Does this raise concerns for you? What, if anything, is the agency doing to remedy the comingling of emails?

Mr. GIBSON. So it raised significant concerns for us when the subject was brought to our attention. Now, it's not all email. There are pockets of email that appear to have been exposed to a program that enables it to be searched. In fact, it was discovered in the FDIC's search of its email vault in response to this Committee's request for information. They are emails that involve certain members of our staff that involve certain periods of time. We've been working closely with the Division of Information Technology at the FDIC to identify the emails that are there, to segregate them, to prevent them from being found through the course of the use of that. We're looking at logs to determine who's looked at those emails. We're conducting a good deal of independent work to provide ourselves with as much assurance as we can about the security of that stuff. I'd be happy to describe that in more detail. I don't want to take all of your time.

Mr. HULTGREN. No, I'd like to hear more about it. I mean, this is really the focus of my question. So I mean, if—and really, what we can do. I'm concerned about this. Again, I think is an important service tool, something that we need, and so I'm concerned of some of the—what I see as negative impact that could come from this, so I'd love to hear from you suggestions of what we can do, what you're doing to make sure that your work is protected and the integrity is strong.

Mr. GIBSON. One of the things that we are doing is we're bringing in an independent group to advise us, you know, and to provide us with independent assurance that the steps that have been taken to mitigate this issue are correct, that the search logic and the search efforts that we have undertaken to be sure that we know exactly the scope of all of the problems that we have have been fully identified and again remediated.

I think that on a longer-term basis, what this leads us to is questioning where our IT environment should be located. We want to take our time in answering that question because obviously there are large implications for our office both from a staffing standpoint and a financial standpoint, if nothing else but balancing that against the need for at least the outward aspects of independence that are implicated when the suggestion can be made that somebody's taking a look at email. There's a lot of issues for us to balance in this, and we're trying to do it quickly, but we want to be sure we do it in a very thoughtful manner.

Mr. HULTGREN. I appreciate that. We certainly want that, but we also want to hear from you as you are coming to conclusions of how do we do this well, how do we make sure that we're assisting in this again to make sure that as best as we can the information we're getting from your office we know isn't affected, compromised, being seen before we have a chance to——

Mr. GIBSON. Absolutely, sir, and we completely understand and agree with that, and I'll be more than happy to provide you or staff with whatever information we can as we move through this process just to keep you updated on the things that we're doing and what we think that we need to do.

Mr. HULTGREN. Great. Thank you.

With that, I yield back, Chairman. Thank you.

Mr. LOUDERMILK. I thank the gentleman.

Mr. Gibson, thank you for that. I think that shows foresight and planning and being proactive, not just reactive to these types of steps, and I think that's the type of thing that we would be looking for.

With that, I recognize the gentleman from California, Mr. Rohrabacher, for five minutes.

Mr. ROHRABACHER. Thank you very much, Mr. Chairman, and let me apologize. Earlier on in the hearing, I was at a markup, and quite often we have two or three responsibilities happening at the same time, so maybe I'll try to go to more of a—rather than go into details, I could get some analysis view of the actual basis, the fundamental issues of what we're talking about.

We're discussing computers that were hacked by the Chinese or other entities between 2010 and 2013 of the Federal Deposit Insurance Corporation. What harm could come of the fact that you have other entities and the Chinese hacking into your computer system? What harm would that cause?

Mr. GIBSON. Sir, is that question directed——

Mr. ROHRABACHER. Whoever.

Mr. GIBSON. It can cause significant harm obviously. I mean, there's a significant volume of information that's available in the FDIC's IT environment, a great deal of sensitive information, whether it's privacy-related information or information related to——

Mr. ROHRABACHER. Maybe you can give me an example of something harmful that could come from that.

Mr. GIBSON. Well, for example, there are large volumes of information about specific financial institutions. Let's take just the Dodd-Frank resolution plans. There are non-public segments of those documents. That information could be extremely valuable to an adversary, and it may be something that could be targeted by someone.

Mr. ROHRABACHER. So if we have Chinese hacking into our system, what you're saying is that because they were—this was happening, perhaps American businesses that are doing business here and in China who are facing competitors or facing adversaries, economic adversaries, that the American companies because we are complying with the information required of us by the Federal Government could be put in economic jeopardy?

Mr. GIBSON. Sir, in theory, there's risk there, yes.

Mr. ROHRABACHER. All right. So this really could add up to very great harm done to Americans financially, both American companies, perhaps some individuals as well who have invested in those companies.

Now, we're being told that of course now that the FDIC was less than forthcoming about this. Now, I seem to remember those days.

We were told over and over and over again about the importance of not getting—of being hacked into and cybersecurity was something we talked a lot about, but yet we now are, from what I've heard even now and read so far about the hearing is the FDIC was less than forthcoming to Congress about what was going on, and in fact, we were not informed and intentionally uninformed of this.

So let me just note for the record, Mr. Chairman, that this attitude that we're talking about that pervaded, that actually made people make their decisions based on an attitude that prevailed at the FDIC is, number one, of course something that is unacceptable, but I see that as part of a trend in this Administration.

Listen, I worked in the Reagan White House and it was very, very clear that what happens at the very highest level of an administration creates the attitude and the standards that go right on down to the departments and agencies. So let me just suggest, and what I've heard so far, and what this indicates is that there's been a pattern of obfuscation in this Administration, not only on this issue but others. There's been a pattern of stonewalling and covering up mistakes and wrongdoing, and these things cannot be just shrugged off. These are things that have to be taken seriously, especially when as we are noting now that there is actual damage to the American people where actually some people we could have billions of dollars' worth of financial harm done by information that's supposed to be secret information, confidential information, but is now being ignored when our economic enemies actually get their hands on the information.

I would suggest that we have here is not a culture of secrecy at your department but instead a disrespect for Congress's right of oversight, a disrespect for the rights of the American people to actually get the information during Congressional hearings, and so what we've had is from the beginning a cover-up and obfuscation of that cover-up of not necessarily wrongdoing but covering up the fact that somebody wasn't maybe able to do their job. You can't expect things to be corrected if it's done even with a good motive, but if you have some evil motives going on, that will never be uncovered unless we have better cooperation between the executive branch and the legislative branch, especially in oversight responsibilities.

So thank you very much, Mr. Chairman, for your oversight responsibilities.

Mr. LOUDERMILK. I thank the gentleman from California, and I think it's imperative for us to understand that, you know, the American people rely upon this government for their safety and security, from homeland security to even the safety and security of their financial assets through the FDIC. The frustration with the American people is that because of multiple incidences, they rely on the government but their trust in the government is at an all-time low, and it's because of situations such that Mr. Rohrabacher has spoken about and what we're investigating here.

With that, the Chair recognizes the gentleman from Arkansas, Mr. Westerman, for five minutes.

Mr. WESTERMAN. Thank you, Mr. Chairman. I'd also like to extend my appreciation to Mr. Gibson for their work. If I could ask the Committee staff to put a slide up? Okay. Thank you.

[Slide]

I just want to read from the transcript. This is an except, some questions and answers. The first question was, "Were those updates being provided to anyone in the Chairman's office or the Chairman himself" and the answer was "Let's see. At the time it was Roddy, Brian, myself, Martin, Chris, and Russ Pittman. The COO was later added." The question is, "Is that Barbara Ryan?" and the answer was, "On December 1st." Question: "Barbara Ryan is the COO and chief of staff to the chairman. Is that correct?" The answer is "Yes." The next question: "Does she act as the chairman's eyes and ears in meetings like this?" and the answer was, "My understanding—I don't have direct knowledge of that but yes."

So Mr. Gruenberg, did you attend meetings regarding the cybersecurity incidents including the Florida incident to discuss the agency's response to the breaches?

Mr. GRUENBERG. I believe, Congressman, I was briefed on November 19th by the CIO in regard to the Florida incident, and I think that was the only briefing I actually had on it.

Mr. WESTERMAN. So you actually didn't attend——

Mr. GRUENBERG. No, sir.

Mr. WESTERMAN. Okay. So when you were not present, did your chief of staff, Barbara Ryan, attend?

Mr. GRUENBERG. As indicated in the—I believe so, yes.

Mr. WESTERMAN. And how often did Barbara Ryan brief you on the status of the breaches?

Mr. GRUENBERG. She really didn't brief me, as it were. There may have been occasions where she gave me a heads up but not—it wasn't really her role to do the briefings.

Mr. WESTERMAN. Even though the transcript says she was your eyes and ears?

Mr. GRUENBERG. Well——

Mr. WESTERMAN. Maybe she really wasn't your eyes and ears?

Mr. GRUENBERG. I don't know how to characterize that but in terms of an actual briefing on these matters, she wouldn't have been the one to do it.

Mr. WESTERMAN. Okay. So the Committee understands that based on the Inspector General's report that the FDIC failed to notify Fin-Syn that Bank Secrecy Act information was involved in the Florida breach until prompted to do so by the Inspector General. Why did the FDIC not notify Fin-Syn of the breach?

Mr. GRUENBERG. I think we should have. I think we failed to do so in that instance, Congressman.

Mr. WESTERMAN. And the Committee now understands that the FDIC has in fact notified Fin-Syn yet you approved the notification to Fin-Syn. Why do you have elevated concern when it comes to notifying another agency within the executive branch of a breach yet opted not to report the Florida incident to Congress until prompted by the Inspector General?

Mr. GRUENBERG. I think as we discussed earlier, it was a matter of assessing the incident, and I think what occurred was, there was an assessment that while the incident was a breach, the initial assessment was that it didn't rise to a level of a major incident. When the IG reviewed it and reached a different conclusion and no-

tified us in February, we then adopted the IG's approach to the incident and then reported it as a major incident.

Mr. WESTERMAN. So it took the IG's notification to raise the level of concern enough to actually make the notification?

Mr. GRUENBERG. I think the IG indicated that the approach the agency was taking to assessing the incident was incorrect, and we were using—considering factors relating to risk of harm that weren't appropriate, that weren't really incorporated in the guidance. When that was made clear, we then adopted the IG's approach to applying the guidance and then reported it as a major incident.

Mr. WESTERMAN. Would you say that's an abnormal occurrence or is that—or have things like that happened before where it takes notification from the IG to move forward?

Mr. GRUENBERG. I don't know that I can generalize. I think this was an instance in which a breach occurred, new guidance was issued by OMB, so we were attempting to evaluate and apply the guidance to the breach. I think we frankly didn't get it right, and when the IG made us aware of that, we then complied.

Mr. WESTERMAN. So for each of the Agencies' notifications both to Congress and Fin-Syn regarding the Florida breach, why did the Inspector General have to prompt your agency to report you instead of your staff opting to report the incident to proper entities in real time as it learned of the breach? Are you saying that your staff just didn't understand the seriousness of the breach or the level of the breach?

Mr. GRUENBERG. I think the assessment was that the incident was a breach. I think the initial assessment was that it didn't rise to the level of a major incident, and as I indicated, when the IG provided us analysis to the contrary, we then adopted the IG's approach.

Mr. WESTERMAN. So have there been corrective actions taken so that the staff is trained better or——

Mr. GRUENBERG. Yes, that's one of the recommendations of the IG that we have concurred with and are following through on.

Mr. WESTERMAN. What kind of steps are you taking to make sure this doesn't happen again?

Mr. GRUENBERG. In addition to as a threshold adopting the application of the guidance consistent with the IG's approach, we're incorporating it in policies and procedures to ensure that any incidents like this are reported in a timely way going forward.

Mr. WESTERMAN. And what would you say your confidence level is that if something like this were to happen again that it would be reported without the IG having to get involved?

Mr. GRUENBERG. I think at this point I have a pretty high confidence level.

Mr. WESTERMAN. Okay. That's all the questions I have, Mr. Chairman. I yield back.

Mr. LOUDERMILK. I thank the gentleman from Arkansas, and we'll begin our second round of questioning, and I recognize myself for five minutes.

Mr. Gruenberg, your CIO, Larry Gross, as you know, testified before my Subcommittee, the Oversight Subcommittee, back in May of this year. At that hearing, Mr. Gross provided this Committee

with false and misleading testimony in multiple incidents about the cybersecurity breaches reported to Congress. For example, I asked Mr. Gross about the Florida cyber breach where an FDIC employee leaving the agency knowingly downloaded over 71,000 counts of personally identifiable information and sensitive bank information onto an external hard drive. She then denied owning the external hard drive, claimed she did not download the information, and refused to cooperate with FDIC officials and OIG officials trying to recover the hard drive.

Ultimately, three months after she took the information, the breacher hired an attorney to negotiate with the FDIC over the return of the hard drive with the information on it. Mr. Gross told the Committee that in his opinion, the breacher was "telling the truth," and Mr. Gross said, "I don't believe she realized she took FDIC-specific data."

We now know that this was not true, and Mr. Gross knew at the time that this was not true. Mr. Gross also claimed in the hearing that "the individuals involved in these instances were not computer proficient," which we also know to be false. In fact, the Florida incident breacher held two master's degrees in information technology, which I think any reasonable person would consider that to be proficient in computer technology.

This Committee wrote to you a letter on May 19, 2016, articulating these misleading statements and more that Mr. Gross made at that hearing. Mr. Gibson, can you corroborate of those statements that were made in the May hearing by Mr. Gross and their inconsistencies?

Mr. GIBSON. Sir, I believe you've described accurately what was said during the hearing, you know, as well as the facts that surround the statements themselves.

Mr. LOUDERMILK. Thank you for that.

Mr. Gruenberg, your response to our letter did not address any of these inconsistencies. With that, Mr. Gruenberg, do you condone Mr. Gross, your CIO, lying to Congress?

Mr. GRUENBERG. Congressman, I can share with you my perspective on it for——

Mr. LOUDERMILK. Please do.

Mr. GRUENBERG. As I indicated earlier, I think Mr. Gross was assessing the facts of the situation relating both to the inadvertence of the employee taking the information as well as the issue of her proficiency. It's my understanding and belief that the conclusions he reached were sincerely reached.

Mr. LOUDERMILK. But Mr. Gibson was here at that testimony and just corroborated that Congress was misled and that the information that Mr. Gross provided this Committee was inconsistent. Do you—so you do not believe that he misrepresented the information or misled the Committee through his testimony in May?

Mr. GRUENBERG. That was not my perception of it. I was not aware that was the IG's perception.

Mr. LOUDERMILK. Mr. Gibson?

Mr. GIBSON. Sir, what I can say is, I can say that the statements were not—we don't believe the statements were correct. We don't believe they were accurate. Now, we haven't looked at his intent in doing that so I can't answer that. But as far as the accuracy of

the statements themselves goes, I don't believe the statements were accurate.

Mr. LOUDERMILK. And that's what I was getting at. The statements were not accurate. All indications are that he knew different than what he was making a statement to Congress, and to me, trying—I mean, legally when you try to build a false perception, is misleading, which is a form of lying, but you do not believe that that was what Mr. Gross was doing, even with all the evidence that's being presented here and in the letter that was provided to you, which you failed to respond to.

Mr. GRUENBERG. I think the issue is intentionality, and I think if I understand it correctly, the IG's view is that Mr. Gross didn't get it right.

Mr. LOUDERMILK. But the issue is what he said, not his intention. I don't know if he intended to lie to Congress but what he said was not true, and he knew that it wasn't.

Mr. GRUENBERG. Well, I believe—for what it's worth—I believe Mr. Gross thought he was—he was giving you his honest view of the matters. He may have gotten the—he may have gotten it wrong. I don't take——

Mr. LOUDERMILK. So you say that Mr. Gross as the CIO does not consider someone who has two master's degrees in information technology to be computer proficient?

Mr. GRUENBERG. I don't know that he was aware of that at the time, Congressman.

Mr. LOUDERMILK. But then he would make a statement saying that she wasn't computer proficient without having any—it sounds like he's trying to cover something.

Mr. GRUENBERG. I can't—again, I can't speak to his intentionality. I think he believed the woman lacked proficiency.

Mr. LOUDERMILK. And I pressed him on this because he was very consistent in saying he did not believe this was intentionally done. He believed that all instances were not intentional. But yet there were already facts that we found out at the time that were well known. She had hired an attorney. She—I mean, it was obvious that it was intentional, and we found more evidence since then, but yet he consistently said he believed it was unintentional. I just don't see how you get around that he misled Congress.

Mr. GRUENBERG. Well, it's hard for me to speak to what was in Mr. Gross's mind. It was my belief and perception that he was giving you his sincere testimony. It may have been incorrect in terms of evaluating the information. I think he would suggest that there was information on both sides and he reached a conclusion in good faith. I think that's what Mr. Gross would indicate.

Mr. LOUDERMILK. Mr. Gibson, in your opinion, in your investigation, was this breach intentional, the Florida?

Mr. GIBSON. Well, sir, it was described as inadvertent, and I certainly don't see it as inadvertent. You know, I would—the material was downloaded deliberately. The material was downloaded intentionally. There were file structures that were created in order to accommodate it independently. I mean, I'm really not sure how you could—a reasonable person would have to conclude that it was intentional.

Mr. LOUDERMILK. So my understanding was, as this was being downloaded, the lady—the employee created—specifically created folders that read personal and FDIC information, created those folders, which would give an intent that they were intending to download—that's what——

Mr. GIBSON. That's would a reasonable—I think a reasonable person could conclude that, yes.

Mr. LOUDERMILK. Mr. Gruenberg, I understand defending an employee, but if I was in your position, I would be gravely concerned with the testimony that Mr. Gross gave here in light of the advice that he's giving you may not be consistent as well. Do you have any intention of disciplining Mr. Gross for his testimony to Congress?

Mr. GRUENBERG. I think, Congressman, in light of the issues you raised, we will review this situation.

Mr. LOUDERMILK. Well, I appreciate that.

With that, I recognize my good friend, the gentleman from Virginia, Mr. Beyer, for five minutes.

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

Mr. Gruenberg, I built a Land Rover-Range Rover dealership across the river, and seven, eight years ago, one of my Land Rover technicians stole all of our customer records, and he went out and opened his own business, and he had a running start because he was able to market to all of them. I could never prove it in a court of law so I just got to be angry about it. But it did make us go back and think about all of our password protections and changing it every 30 days and the like. What was going on in the culture at FDIC that would lead employees to download records and take them home? They're clearly not going to start a competing FDIC.

Mr. GRUENBERG. I can't, you know—we had a number of these incidents that were similar in their fact pattern where employees were leaving the agency, they had utilized removable media, downloading personal information and downloading in addition sensitive information from the agency. I don't know if there was any connecting pattern there. I don't know that I can speak to that. It did—it does speak obviously to an underlying technological vulnerability we had relating to permitting employees to use their removable media, and that's at least what we've tried to address.

Mr. BEYER. Thank you. There was a slide up earlier about the transcribed interview with another FDIC employee. It talked about directions from Roberta McInerney about not creating an email record. I understand the Majority staff had set up an interview with Ms. McInerney and then had to cancel it. Are you aware of any ongoing efforts that will be made to actually interview Ms. McInerney and try to get to the bottom of why she did this?

Mr. GRUENBERG. It's my understanding that the interview was postponed. I can't speak to whether it'll be rescheduled or not.

Mr. BEYER. Any sense of the consequences from the top for Ms. McInerney for giving these directions?

Mr. GRUENBERG. I think we'll have to review the circumstances here.

Mr. BEYER. Okay. Certainly, from a good government, transparent government perspective, if true, it's pretty terrible stuff.

The OIG and some in the CIO's own office disagreed with the CIO's initial determination that the Florida incident wasn't a

quote, unquote, major incident, but then after the February 19 OIG memo recommending the breach be determined major and immediately reported to Congress, you did that within 7 days. In fact, the CIO had said that the FDIC agreed to abide by the OIG's interpretation of a major incident as defined in OMB memo 1603.

However, one of the recent major incidents, the one on March 26, 2016, wasn't reported to Congress for 5 weeks until May 9, 2016, which is well after the 7-day reporting requirement, well after you'd agreed that the OMB memo made sense. Can you explain the delay in Congressional notification, and do we have your assurance that data breaches determined to be major will be reported within the 7-day time period?

Mr. GRUENBERG. Yes, you certainly do, Congressman.

Mr. BEYER. Any idea how to explain the 5-week breach from March 26 to May 9? Because this is significantly later than the October incident last year.

Mr. GRUENBERG. I think—I have to go back and check for sure. We were also checking the record for the breaches going back to October 30, whether other breaches had occurred, and we were identifying additional breaches, and I think the thought was to aggregate them and bring them together and report them at one time to Congress so they'd have the benefit of all of them. In retrospect, we probably should have just gone ahead with the 7-day.

Mr. BEYER. Because it's easier to explain the October one where it was initially identified as not major than to explain and to justify the later ones.

Mr. Chair, I yield back.

Mr. LOUDERMILK. I thank the gentleman from Virginia, and the Chair recognizes the gentleman from Louisiana, Mr. Abraham, for five minutes.

Mr. ABRAHAM. Thank you, Mr. Chairman.

Mr. Gruenberg, I think in this hearing and the other hearings that I've attended in Congress, if I had a dollar for every time I heard the phrase "I'll review and get back to you," I could significantly pay down the national debt.

I've got a letter that I'll ask to submit for the record, Mr. Chairman, that Mr. Gruenberg wrote to you and Chairman Smith May 25, 2016.

Mr. LOUDERMILK. Without objection, so ordered.

[The information appears in Appendix II]

Mr. ABRAHAM. Mr. Gruenberg, in this letter, you wrote that Chairman it was discussing the major incidences that you have not reported to Congress. In your letter, you wrote, and I quote, "In each instance, the information was recovered and there was no evidence of further dissemination or disclosure." Do you stand by that statement in the letter?

Mr. GRUENBERG. Yeah, I believe we have no evidence of further dissemination, yes, sir.

Mr. ABRAHAM. Well, I may disagree a little bit. Isn't it true that at least one of the cases you were only able to recover a copy of the USB that was taken off premise?

Mr. GRUENBERG. Yes, in one case the original——

Mr. ABRAHAM. You didn't get the original back?

Mr. GRUENBERG. Correct. It had been destroyed.

Mr. ABRAHAM. So really, you didn't recover all the evidence?

Mr. GRUENBERG. Oh, we recovered—there was a copy made and we did——

Mr. ABRAHAM. But we still got something out there possibly?

Mr. GRUENBERG. We do. That's—you know, that's why you can't say with certainty that there was no dissemination. We just haven't identified any.

Mr. ABRAHAM. Mr. Gibson, what's your take on this?

Mr. GIBSON. Well, sir, in—I have to think through the incidents themselves. In at least——

Mr. ABRAHAM. Well, let's just take this one case.

Mr. GIBSON. In that one case, you know, the individual took the USB drive when they left the agency. They copied the data off of it at some point in time, destroyed the original USB drive——

Mr. ABRAHAM. Do we know that it was destroyed?

Mr. GIBSON. No, we don't. There's no assurance——

Mr. ABRAHAM. That's a major concern to me. I mean, I can tell you one thing, but doing something is a whole different——

Mr. GIBSON. Yeah. No, it was done in a manner where there really isn't any assurance of what happened to it. I mean, there was no receipt for it. It was given to a third party to destroy. There was no receipt. There's no record at the company of the destruction. There's no way for us to verify independently that it was done.

Mr. ABRAHAM. And clarify for me, has it now been stopped, a development of a program that would detect these insider threats? Is that where we're at now that we are not developing a program? Where does that stand?

Mr. GRUENBERG. That's one of the recommendations of the IG's report, and we've concurred with it and are in the—we have been developing the program and we anticipate bringing it to a conclusion and implementation by the end of this year, I believe, Congressman.

Mr. ABRAHAM. I mean, it just—it's beyond the pale that we wouldn't want to detect an insider threat.

Mr. GRUENBERG. Right. No, no it's——

Mr. ABRAHAM. Certainly after Mr. Snowden's major episode.

I yield back, Mr. Chairman. Thank you, sir.

Mr. LOUDERMILK. I thank the gentleman, and also I would like to thank the Office of the Inspector General for the two reports recently issued on this, the FDIC's control for mitigating the risk of unauthorized release of sensitive resolution plans and also the FDIC's process for identifying and reporting major information security incidents. We thank you for your work on that, and without objection, I would like to submit these for the record.

Without objection, so ordered.

[The information appears in Appendix II]

Mr. LOUDERMILK. I also look forward to Mr. Gruenberg responding to the numerous questions and requests in a timely manner to the Committee because this is an ongoing investigation and we'll continue to investigate and research the facts in this matter in the coming weeks and months, and I thank both witnesses, Mr. Gibson and Mr. Gruenberg, for being with us today. I thank our Members of the Committee for their very important questions.

And just a reminder that the record will remain open for two weeks for additional comments and written questions from Members.

Mr. LOUDERMILK. And with that, this meeting is adjourned.

[Whereupon, at 12:17 p.m., the Committee was adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by The Hon. Martin J. Gruenberg

Response to questions by Congressman Don Beyer
from Martin J. Gruenberg,
Chairman, Federal Deposit Insurance Corporation

Q1: In 2010, FDIC's computers were penetrated by an "Advanced Persistent Threat" (APT). The FDIC Office of Inspector General (OIG) investigated this breach in a report it issued in 2013. Some of the FDIC's senior IT security officials at the time failed to inform either the IG's office or senior FDIC officials, including you, about this penetration and its significance. At the July 14 hearing you were informed that one FDIC employee testified that you were supposedly not told about this penetration at the time because of concerns regarding your confirmation hearing to become the FDIC Chairman. Please take this opportunity to more fully describe when you first became aware of the 2010/2011 cybersecurity attack, who informed you of this incident, when you became aware that this information was not shared with you and other senior FDIC officials, and what specific actions you took both procedurally and against specific personnel to hold individuals accountable and to improve FDIC's cybersecurity posture.

A1: I first became aware of the cybersecurity attack on August 26, 2011, during a briefing by our Chief Information Officer (CIO) and Division of Information Technology (DIT) director Russell Pittman, and Chief Information Security Officer (CISO) Ned Goldberg. The briefing provided a general summary of the security issue and suggested that the matter was a routine computer security event and was contained. I received no subsequent briefings on the topic until March 2013 when the FDIC Office of Inspector General (OIG) notified me that the incident had not, in fact, been contained in 2011 and that DIT had found it necessary to continue to address the intrusion since that time. The OIG conducted an investigation of the incident and provided their report to me on May 24, 2013. I learned from this report that DIT failed to fully inform me, other Board members, and the Chief Risk Officer of the severity and magnitude of the intrusion, did not report the incident in any meaningful way to US-CERT, and failed to adequately disclose the incident to the Government Accountability Office and the FDIC OIG.

In response to these events, the FDIC realigned its IT organizational structure and major functions to enhance accountability and eliminate potential conflicts among key roles. The positions of CIO and DIT director were separated, with the CIO to report directly to the Chairman, and the DIT director to the CIO. The information security and privacy unit was moved out of DIT and established as a separate entity reporting to the CIO. The CISO left the agency in 2013 and the responsibilities of the DIT director were curtailed. Finally, the FDIC established a senior-level committee chaired by the Chief Operating Officer that meets monthly to assess cyber security threats and developments impacting both the FDIC and the banking industry.

The FDIC also contracted with an outside cybersecurity firm, Mandiant, to determine if the incident was ongoing and to assist the FDIC in hardening our environment against any future attack. Mandiant delivered a report in September 2013 that concluded "no evidence of ongoing attack activity was identified during Mandiant's investigation." Due to a lack of evidence of ongoing attack activity or compromised systems, Mandiant could not tailor its remediation

recommendations based on investigative findings. Instead, Mandiant recommended that the FDIC evaluate the feasibility of implementing a set of 23 recommendations that apply to most victims of targeted attacks.

The FDIC evaluated and began implementing 18 of the 23 items Mandiant recommended. Three of the 23 were already in place, and two could not be implemented in the FDIC environment. Eleven of the 18 recommendations the FDIC pursued have been completed, and the remaining seven required significant change and are still in process. However, material progress has been made on those seven and the FDIC has implemented mitigating controls and protections to lower risk while all necessary actions are completed.

The FDIC has improved the information security and privacy program in several ways beyond the Mandiant recommendations. For example, we have added seven permanent staff to the information security and privacy team.[4] We also have implemented or extended tools that help protect our sensitive information such as the Data Loss Prevention tool and a tool deployed to PCs that detects unauthorized software. We also have deployed new protective tools at our firewalls to prevent external threats from gaining access to our systems.

[4] In two of these cases, a temporary position was replaced with a permanent position.

Response to questions from Congresswoman Eddie Bernice Johnson
from Martin J. Gruenberg,
Chairman, Federal Deposit Insurance Corporation

Q1: At the July 14 FDIC cybersecurity hearing the Majority suggested that establishing "Digital Rights Management" technologies at the Federal Deposit Insurance Corporation (FDIC) would render the Agency's use of its current Data Loss Prevention (DLP) software ineffective. Digital Rights Management (DRM) technologies generally refer to a mix of technologies that can prevent files from being copied, shared or altered. DRM software can also be used to provide a specified window of time in which a particular recipient may be granted access to certain data or files. On the other hand, DLP software is used to alert information technology (IT) security officials when particularly sensitive data is sent to an e-mail address outside an Agency or organization, printed, or downloaded to removable media, such as a thumb drive, for instance. In one of the Majority's "transcribed interviews," a FDIC cybersecurity expert made clear that DRM is "a great tool" that "would actually integrate with a data loss prevention tool." In addition, commercial IT security companies, including Symantec, Adobe and McAfee all suggest using DRM in combination with DLP software. Suggesting that employing DRM would "render DLP ineffective," does not appear to be accurate. However, there have been concerns about how FDIC will integrate these two tools together to be most effective.

Can you please indicate what steps are being taken to ensure that DRM will be integrated effectively with FDIC's DLP software and does not have the unintended consequence of diminishing FDIC's cybersecurity tools already in place.

A1: The FDIC has researched solutions that claim to directly integrate DLP and DRM software, and researched possible FDIC integrations that could ensure DLP and DRM software function effectively, without degrading one another.

For example, makers of DLP and DRM software make claims of software integration so that DLP tools can review the contents of a DRM-wrapped file. Some of these tools are not yet on the market, but are promised soon. The FDIC has researched these solutions and how effective they may be in our environment.

Separately, the FDIC is researching DRM deployment options that would allow DLP tools to review files before they are "wrapped" by DRM tools. This approach, in theory, would allow both tools to operate effectively. Our research is ongoing, as is the maturing of these toolsets by the commercial vendors that sell them.

We are engaging an outside firm, Booz Allen Hamilton, to review these potential solutions and provide us with an evaluation as part of an overall review of our information security and privacy program. The evaluation will inform us on any decision made on this issue.

Q2: The impetus for the first Science Committee hearing on FDIC data breaches was held on May 12, 2016 and looked at a series of breaches related to removable media and departing employees. What actions have the FDIC taken to prevent data breaches related to removable media and FDIC employees? Specifically, what actions have been taken since the first hearing—on May 12, 2016—and are other actions to enhance FDIC's cybersecurity procedures planned?

A2: The FDIC has discontinued individuals' ability to copy information to removable media such as: external hard drives, flash drives, and CDs or DVDs, to prevent these types of incidents from occurring. Exceptions are currently limited to 2 on-site Government Accountability Office employees, 72 OIG employees, and 5 FDIC Legal Division employees (as necessary for litigation, FOIA, or Congressional requests that may necessitate removable media usage).

Additional actions to enhance FDIC's cybersecurity procedures are being implemented.

- The FDIC is revising policies and procedures such as the "Data Breach Handling Guide," and the policy circular titled "Reporting Computer Security Incidents," to better specify what actions should be taken when an incident occurs.
- The FDIC is reviewing the Data Loss Prevention tool implementation to determine how the tool can be better leveraged to safeguard sensitive information.
- The FDIC is strengthening testing of technical information security controls to confirm that the controls operate as intended.
- The FDIC is adding an information security professional position to an office that works with sensitive information.
- The FDIC will be engaging with an independent firm, Booz Allen Hamilton, to evaluate our overall information security and privacy program. That company's evaluation began August 1, 2016, and will be completed in October 2016.
- The FDIC is completing implementation of a new incident tracking system that will more centrally organize incident facts and enhance incident response management.
- The FDIC is implementing a formal insider threat program.

These are examples of a number of actions we are taking, or are planning to take, to enhance FDIC's cybersecurity program.

Response to questions by Congressman Mo Brooks
from Martin J. Gruenberg,
Chairman, Federal Deposit Insurance Corporation

Q1: Does the FDIC employ the standard protections: full-disk encryption on all personal machines, remote management of security (not user-configured security), two-factor authentication, etc.?

A1: FDIC laptop hard drives are encrypted using a commercially-available solution that is consistent with NIST encryption standards.[1] FDIC desktop hard drives are not encrypted but are located within secured FDIC premises with cases that are locked such that non-authorized employees are unable to physically access the hard drives. The FDIC is evaluating the replacement of desktops with laptops.

To help protect sensitive email, the FDIC also provides email encryption solutions. One solution is used for sensitive email exchanges with parties outside the FDIC and a second solution is used to encrypt sensitive internal emails.

FDIC personal computers (PCs)[2] are managed by information technology administrators, not the end users. End users are limited in what they are able to change on PCs because they do not have operating system administrator privileges. PCs also have standard software configurations that are periodically updated with automated tools.

Two-factor authentication is currently required to access the FDIC network from PCs outside the FDIC network,[3] and in most instances to access the network internally if the individual is a privileged user. The FDIC is migrating from a physical token for two factor authentication to Personal Identification Verification (PIV) cards. Once PIV cards are deployed, the FDIC will incrementally change the environment so that PIV cards are required for FDIC employees and contractors to access FDIC information technology resources from anywhere.

Other protections and controls are deployed to FDIC's PCs such as: anti-virus, host-based intrusion prevention, data loss prevention, and application whitelisting software.

Additionally, the FDIC utilizes protections for the BlackBerry and Apple smart phones and tablets it provides to a subset of employees. Both BlackBerry and Apple devices have encrypted containers that protect FDIC sensitive information on the devices. These devices are ID and password protected and the FDIC is exploring two-factor access solutions that could be added to these devices.

---

[1] Federal Information Processing Standard (FIPS) Publication 140-2, common criteria EAL4.
[2] Personal computers refers both to laptops and desktops.
[3] For example, FDIC examiners connecting to the FDIC network from a commercial cellular network while working at a bank.

Q2: What is the FDIC's risk management strategy?

a. **What process does the FDIC use for evaluating the most important data to secure?**
b. **How does the FDIC information security strategy then allocate resources to accordingly protect those resources?**

A2: The FDIC's risk management strategy is to ensure assets are well-identified and categorized, and that controls are deployed to protect assets based on their value or level of sensitivity.

The FDIC maintains asset inventories (systems, hardware, and data) and currently uses the National Institute of Standards and Technology's (NIST) Federal Information Processing Standard 199, "Standards for Security Categorization of Federal Information and Information Systems," to categorize assets. Assets are categorized with regard to their confidentiality, integrity, and availability requirements (CIA). Additionally, the FDIC recently completed a review of our systems based on the Office of Management and Budget's (OMB) High Value Asset (HVA) definition, and provided a list of the top 18 HVA systems based on that review to the Department of Homeland Security. The FDIC is reviewing these systems and their associated business processes in light of OMB guidance to determine if additional controls are required.

When systems are created, the system hardware and data CIA ratings are evaluated to characterize the system as a whole and determine the appropriate NIST baseline controls to apply. Factors such as whether the system contains sensitive PII or sensitive business information, whether it is Internet-facing, whether it is a financial system, and whether it is mission critical also impact the security scrutiny it receives. Systems are also classified as either major or minor based on their importance to the FDIC's mission, finances, management visibility, and other impact categories. Those systems rated as major receive the most significant security scrutiny and resource allocation.

Finally, the FDIC has a continuous monitoring program based on NIST's Risk Management Framework and on NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems." The FDIC's continuous monitoring methodology consists of five essential components:

1. configuration management and change control,
2. an information security risk management program,
3. a Security Impact Analysis,
4. security status monitoring and reporting, and
5. active involvement of FDIC officials.

This five-part program produces a regularly updated inventory of information security improvement tasks that are prioritized based on risk, and completed with oversight by the Chief Information Officer (CIO).

Q3: What methods have you employed to ensure that your security protections work?
- **a. Do you employ red teaming?**
- **b. If you have engaged in red teaming, what were the rules? Could the red teams engage in social engineering? Did the red teams have to operate within the law in conducting the attacks against your systems?**

A3: Yes, the FDIC contracted in both 2015 and 2016 with an independent, third-party company to perform adversary simulations ("red teaming") to identify weaknesses in its security posture.

The rules for the simulations were that the company could target any FDIC system and use any credentials they could access. Social engineering and denial of service attacks were out of scope. The testers used methods that would be illegal if they were not specified in the contract. The company exploited vulnerable systems and misused exposed credentials using methods similar to criminal hackers.

In addition, the FDIC maintains an ongoing contract with a company to regularly test both FDIC employees and contractors for susceptibility to phishing exploits. Employees and contractors who fail these tests are directed to training material to enhance their ability to spot phishing attacks in the future.

Finally, the FDIC participates in the DHS-sponsored Cyber Hygiene assessment on a weekly basis to help identify any weaknesses and improve security in Internet-facing systems.

Responses by Mr. Fred W. Gibson

QUESTIONS FOR THE RECORD
The Honorable Mo Brooks (R-AL)
U.S. House Committee on Science, Space, and Technology

Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information

Thursday, July 14, 2016

Questions for Mr. Gibson

1. Does the FDIC employ the standard protections: full-disk encryption on all personal machines, remote management of security (not user-configured security), two-factor authentication, etc.?

Full-Disk Encryption on Personal Machines

The FDIC has a highly mobile workforce and, as such, the majority of its employees use FDIC-furnished laptop computers to support their work activities. The FDIC uses a full-disk encryption software product called PointSec for PC (PointSec) to encrypt the contents of laptop hard drives, including software applications, data, office documents, system files, temporary files, and deleted files. The encryption process runs automatically in the background and is transparent to the user. PointSec is not configured to encrypt email communications or data stored on other IT platforms, such as shared network drives. The FDIC employs different solutions that may be used by employees or contractor personnel to encrypt emails and data stored on other IT platforms.

Some FDIC employees use FDIC-furnished desktop computers. Although these employees have the ability to manually encrypt individual data files stored on their desktops, the FDIC has not deployed a solution that automatically encrypts data and applications on the desktop computers. In addition, emails and other data accessed from network shared drives through a desktop computer are not automatically encrypted, but can be encrypted as described above.

For many years, the FDIC has authorized its employees to use FDIC-furnished BlackBerry devices for business purposes. Data stored on BlackBerrys is encrypted. However, BlackBerry devices cannot read emails that are encrypted using the FDIC's email encryption solution. Recently, the FDIC began to pilot test Apple iPhones as a replacement for BlackBerrys. We have not reviewed the configuration of the iPhones to determine the extent to which data stored on them are encrypted.

The FDIC has also authorized the use of FDIC-furnished Apple iPads for its executive managers. We have not reviewed the configuration of these tablet devices to determine the extent to which data stored on them are encrypted.

Remote Management of Security

The FDIC owns and centrally manages the laptop and desktop computers connected to the corporate network. Administrators in the Division of Information Technology (DIT) perform security and configuration management of laptops and desktops. General network users do not have administrative privileges to configure their laptop and desktop computers.

The FDIC's laptop and desktop computers are configured with a standard image that is periodically updated by DIT. Configuration changes and software patches are pushed to these computers by DIT using automated tools, and the computers are periodically reviewed and scanned for security vulnerabilities and compliance with FDIC security policies by the Chief Information Officer (CIO) Organization.

The FDIC is currently considering contracting with a service provider that would deliver a mobile device management solution and services for all mobile devices. The provider would be responsible for delivering, securing, and managing the FDIC's mobile devices and applications across the enterprise.

Two-Factor Authentication

The FDIC requires both privileged[1] and non-privileged users to use multifactor authentication (MFA) when accessing the FDIC's network remotely. In addition, privileged users have used a token-based MFA solution to access the network from within FDIC facilities since 2014. Non-privileged users, however, do not currently use MFA to access the network from within FDIC facilities.

In September 2015, the FDIC made a decision to implement a token-based MFA solution for its non-privileged users who access the network from within FDIC facilities. In early 2016, the FDIC shifted direction on this effort and decided to instead implement a Personal Identity Verification (PIV) card-based MFA solution for both privileged and non-privileged users of the network. This change in direction was prompted by the issuance of the Office of Management and Budget's (OMB) Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, dated October 30, 2015, which directed federal agencies to issue and use PIV cards for MFA.

The FDIC is currently working to issue PIV cards to its employees and contractor personnel to enable the use of the new PIV-card MFA solution. The FDIC expects that the vast majority of its employees and contractor personnel will have PIV cards by the end of September 2016. The FDIC plans to begin enforcing the use of PIV cards to authenticate to the network in 2017. We continue to monitor the FDIC's progress in this regard.

2. What is the FDIC's risk management strategy?

    a. What process does the FDIC use for evaluating the most important data to secure?
    b. How does the FDIC information security strategy then allocate resources to accordingly protect those resources?

FDIC Circular 1310.3, *Information Security Risk Management Program*, dated March 9, 2015, defines the FDIC's policy and approach for identifying, evaluating, and managing security risk to the Corporation's information systems, services, and associated data. The circular defines a 3-tiered approach for managing risk at the organization level, mission and business process level, and information systems level. A key component of the FDIC's risk management program is an Information Security Risk Advisory Council comprised of the FDIC's CIO, Chief Risk Officer, and Chief Information Security Officer (CISO). This council is responsible for (among other things)

developing a corporate security risk tolerance level and risk profile, which are to be used to prioritize risk management activities. In addition, the FDIC is working to update its *Business Technology Strategic Plan 2013—2017*, which includes a component on information security.

a. What process does the FDIC use for evaluating the most important data to secure?

Historically, the FDIC has assigned impact ratings of high, moderate, or low to its information systems and data as prescribed by the National Institute of Standards and Technology's Federal Information Processing Standard Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated February 2004. The three impact ratings reflect the potential effect on the FDIC or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). More recently, and in response to the 30-day Cybersecurity Sprint initiated in June 2015 by the United States CIO and subsequent guidance issued by the OMB in October 2015,[2] the FDIC identified and provided to the Department of Homeland Security a list of its high value assets (i.e., those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries).

To identify its high value assets, the FDIC's Information Security Risk Advisory Council (described above) compiled existing lists of sensitive information, including both business sensitive information and personally identifiable information. This cumulative list was then provided to the FDIC's Information Security Managers, who are responsible for information security in each of the FDIC's business areas, for review and revision. The results of this effort were used to develop a draft list of high value assets, which was then provided to the FDIC's division and office directors for final confirmation before the information was submitted to the Department of Homeland Security.

b. How does the FDIC information security strategy then allocate resources to accordingly protect those resources?

We have not performed independent work in recent years to assess how the FDIC's information security strategy allocates resources to protect the Corporation's IT resources. However, we note that the FDIC has various processes and committees for allocating corporate resources, including IT and information security resources. These include, for example, the FDIC's IT budget formulation process, the Corporate Budget and Planning Process, the CIO Council, the Capital Investment Review Committee, and the Executive Management Committee.

3. What methods have you employed to ensure that your security protections work?
    a. Do you employ red teaming?
    b. If you have engaged in red teaming, what were the rules? Could the red teams engage in social engineering? Did the red teams have to operate within the law in conducting the attacks against your systems?

The FDIC's CIO Organization has primary responsibility for ensuring that security protections operate as intended. The CIO Organization has engaged a firm to perform technical and security compliance testing of the FDIC's information systems. The FDIC's information systems are subject to an initial technical security assessment (TSA) that evaluates controls as part of the

system's development. Once the system is placed into production, it is subject to a continuous control assessment (CCA) methodology. Major applications and general support systems are evaluated each year, and minor systems are evaluated every 3 years. Security vulnerabilities identified through TSAs and the CCA methodology are documented and tracked in Plans of Action and Milestones. In addition to TSA and CCA activities, the CIO Organization has a vulnerability management program that includes, among other things, regular vulnerability scans of assets connected to the network.

a. Do you employ red teaming?

Red teaming is a process for detecting and analyzing network and system vulnerabilities by modeling the actions of an adversary. The OIG has not performed independent red teaming exercises of the FDIC's network. However, as described below, the FDIC engaged a firm in 2015 to conduct red teaming of its network. An official in the CIO Organization informed us that a separate red teaming exercise is currently underway.

b. If you have engaged in red teaming, what were the rules? Could the red teams engage in social engineering? Did the red teams have to operate within the law in conducting the attacks against your systems?

In 2015, the FDIC's CIO Organization engaged a firm to perform an "adversary simulation" of its externally facing and internal networks from the perspective of an Internet attacker. The assessment was intended to explore relevant risks involved with having systems directly accessible by bad actors on the Internet, as well as to simulate post-breach activities from the perspective of a compromised end-user system. As such, the stated objective of the assessment was to validate preventive and detective controls in the FDIC's IT environment in the event of a targeted end-user compromise, such as a social or phishing attack, a "drive-by" malware infection, or a targeted infiltration aimed specifically at FDIC users and information assets.

The assessment followed a three-phase approach. The first phase consisted of anonymous Internet- based external intrusion attempts, such as attack simulations and breach modeling using malware and tools that a malicious actor might use, and network and Web application penetration testing.
The second phase consisted of simulated post-intrusion activities on the internal network from the perspective of a compromised desktop. This included, for example, analyzing network traffic with the objective of identifying scenarios where the integrity of trusted communications could be diminished or reduced, or the IT environment could be abused, disrupted, or otherwise negatively affected. The third phase involved a vulnerability assessment review and specific technical reviews as requested by the FDIC, drawing from the lessons learned in the first two phases of the assessment.

It does not appear that social engineering was used during the assessment. We did not review the terms of the FDIC's contract with the firm engaged to perform the adversary simulation, so we cannot comment on whether the firm operated within the parameters of the law in conducting its work.

Appendix II

Additional Material for the Record

DOCUMENTS SUBMITTED BY REPRESENTATIVE BARRY LOUDERMILK

Office of Inspector General

Office of Audits and Evaluations
Report No. AUD-16-003

The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans

July 2016

Office of Inspector General

Executive Summary

The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans

Report No. AUD-16-003
July 2016

Why We Did The Audit

Section 165(d) of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act) requires certain financial companies designated as systemically important to report to the FDIC on their plans for a rapid and orderly resolution under the Bankruptcy Code in the event of material financial distress or failure. To implement the requirements of section 165(d), the FDIC and the Board of Governors of the Federal Reserve System (FRB) jointly issued a Final Rule, entitled *Resolution Plans Required*, dated November 1, 2011. The Final Rule requires financial companies covered by the statute to submit resolution plans, sometimes referred to as "living wills," to the FDIC and FRB for review. The resolution plans required by the Dodd-Frank Act contain some of the most sensitive information that the FDIC maintains. Accordingly, safeguarding the plans from unauthorized access or disclosure is critically important to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system.

In September 2015, an employee (referred to herein as "the employee") working in the FDIC's Office of Complex Financial Institutions (OCFI) abruptly resigned from the Corporation and took sensitive components of resolution plans without authorization. The objectives of the audit were to (a) determine the factors that contributed to this security incident involving sensitive resolution plans and (b) assess the adequacy of mitigating controls established subsequent to the incident.

Background

On September 29, 2015, FDIC personnel detected that an employee who had previously worked for OCFI had copied sensitive components of three resolution plans from the network onto an unencrypted Universal Serial Bus (USB) storage device. This activity violated OCFI policy which expressly prohibits the storage of resolution plans on removable media. In addition, the activity appeared suspicious because the information was copied to the USB device immediately prior to the employee's departure. Further, the employee did not have authorization to take any sensitive FDIC information, including resolution plans, upon departure.

Law enforcement officials subsequently recovered the USB device that contained the components of the resolution plans copied by the employee. In the course of doing so, these officials also identified and recovered from the employee a sensitive Executive Summary for a fourth resolution plan that was in hard copy. In early October 2015, OCFI officials coordinated with RMS to notify each of the SIFIs impacted by the incident. In addition, law enforcement officials learned that the employee had interviewed for employment with two of the four SIFIs impacted by the incident following the employee's resignation, suggesting that the employee may have taken the resolution plans for personal gain. Further, there were indications prior to the incident that the employee presented a heightened security risk and may not have been suited to have access to highly sensitive information, such as resolution plans.

The incident involving resolution plans is not an isolated instance of unauthorized exfiltration of sensitive FDIC information by trusted insiders leaving the Corporation. Between February and May 2016, the FDIC notified the Congress of seven major incidents in which employees took significant quantities of sensitive information from the FDIC without authorization when they departed. Individuals that organizations entrust with access to sensitive information pose specific types of security risks to

organizations. Accordingly, special consideration must be given to the risks posed by trusted insiders and appropriate security controls established to mitigate those risks.

Audit Results

We identified a number of factors that contributed to the security incident involving sensitive resolution plans. Most notably, an insider threat program would have better enabled the FDIC to deter, detect, and mitigate the risks posed by the employee. In addition, a key security control designed to prevent employees with access to sensitive resolution plans from copying electronic information to removable media failed to operate as intended. The remaining factors involved OCFI employees having access to resolution plans that exceeded business needs; OCFI's inability to effectively review and revoke employee access to resolution plans because employees were allowed to store copies of the plans outside of the FDIC's official system of record—OCFI Documentum (ODM); and OCFI's inability to monitor all downloading of resolution plans stored in ODM.

With respect to insider threats, the FDIC has a number of long-standing controls designed to mitigate risks associated with trusted insiders. Such controls include, for example, background investigations, periodic inspections of FDIC facilities to identify security concerns, employee non-disclosure agreements, a Data Loss Prevention tool, and programs to help employees cope with personal issues. During 2014 and 2015, the FDIC began to take steps toward establishing a formal insider threat program by, among other things, developing a proposed governance structure and drafting program policies. However, these activities were not completed or approved, and progress toward establishing an insider threat program stalled in the fall of 2015.

Following the incident involving resolution plans, OCFI officials assessed the associated risks and began implementing new or enhanced security controls over resolution plans. Such controls included better aligning employee access to resolution plans in ODM with business needs; increasing the frequency of access reviews for plans stored in ODM; and reviewing employee printing activities to identify and investigate suspicious activity. However, because OCFI had not yet developed written policies, procedures, and assessment plans to govern these new or enhanced controls, we did not have criteria against which to test their effectiveness.

Our report describes additional control improvements that the FDIC should implement to better safeguard sensitive resolution plans. It is important to note that no matter how well designed, implemented, or operated, an internal control system cannot provide absolute assurance that all of management's objectives will be met. Factors outside of management's control, such as a trusted insider who is intent on circumventing internal controls, can affect management's ability to achieve its objectives. Accordingly, the control measures we are recommending are intended to help the FDIC achieve reasonable, not absolute, assurance that sensitive resolution plans are adequately safeguarded.

Recommendations and Corporation Comments

The report contains a total of six recommendations. One recommendation is addressed to the Deputy to the Chairman, Chief Operating Officer, and Chief of Staff to work with other senior FDIC executives to establish a corporate-wide insider threat program. The remaining five recommendations are addressed to either the Chief Information Officer or the Director, OCFI, (as appropriate) to strengthen the FDIC's

information security controls, particularly with respect to safeguarding sensitive resolution plans submitted to the Corporation under the Dodd-Frank Act. The Deputy to the Chairman, Chief Operating Officer, and Chief of Staff; the CIO; and the Director, OCFI; provided a joint written response, dated June 28, 2016, to a draft of this report. In the response, FDIC management concurred with all six of the report's recommendations and described planned actions that were responsive.

Contents

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, Virginia 22226

Office of Audits and Evaluations
Office of Inspector General

DATE: July 6, 2016

MEMORANDUM TO: Barbara A. Ryan
Deputy to the Chairman, Chief Operating Officer, and
Chief of Staff

Lawrence Gross, Jr.
Chief Information Officer

Arthur J. Murton, Director
Office of Complex Financial Institutions

/Signed/
FROM: Mark F. Mulholland
Assistant Inspector General for Audits

SUBJECT: *The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans*
(Report No. AUD-16-003)

This report presents the results of our audit of the FDIC's controls intended to mitigate the risk of an unauthorized release of resolution plans submitted to the FDIC by Systemically Important Financial Institutions (SIFIs) under the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act).[1] The resolution plans required by the Dodd-Frank Act contain highly sensitive, confidential business information that, if compromised, could significantly harm the competitiveness of the institutions involved and the reputation of the FDIC. Accordingly, safeguarding the plans from unauthorized access or disclosure is critically important to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system.

In September 2015, an employee (referred to herein as "the employee") working in the FDIC's Office of Complex Financial Institutions (OCFI) abruptly resigned from the Corporation and took sensitive components of resolution plans without authorization. The objectives of the audit were to (a) determine the factors that contributed to this security incident involving sensitive resolution plans and (b) assess the adequacy of mitigating controls established subsequent to the incident. As part of the audit, we interviewed OCFI and other FDIC officials who were familiar with the circumstances of the incident; assessed key security controls that were established before and after the incident; and identified additional controls that, if implemented, would better position the FDIC to address the risk posed by this type of security incident in the future.

[1] Terms that are underlined when first used in this report are defined in Appendix 2, *Glossary of Terms*.

On July 3, 2014, we issued an audit report, entitled *The FDIC's Controls for Safeguarding Sensitive Information in Resolution Plans Submitted Under the Dodd-Frank Act* (Report No. AUD-14-008).[2] The objective of that audit assignment was to determine whether the FDIC's controls for safeguarding sensitive information in resolution plans submitted under the Dodd-Frank Act were consistent with applicable information security requirements, policies, and guidelines. The report contained seven recommendations intended to enhance security controls over sensitive resolution plan information. Although the FDIC took actions to address all seven recommendations, the security incident in September 2015 revealed additional control weaknesses that are addressed in this report.

We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 of this report includes additional details about our objectives, scope, and methodology; Appendix 2 contains a glossary of terms; Appendix 3 contains a list of abbreviations and acronyms; Appendix 4 contains the Corporation's comments on this report; and Appendix 5 contains a summary of the Corporation's corrective actions.

Background

The FDIC's Information Security Program

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the FDIC, to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support the operations and assets of the agency. FISMA directs the National Institute of Standards and Technology (NIST) to develop risk-based standards and guidelines to assist agencies in defining security requirements for their information systems. NIST documents and communicates required security standards within Federal Information Processing Standards Publications and recommended guidelines within Special Publications (SP). NIST publications provide federal agencies with a framework for developing appropriate confidentiality, integrity, and availability controls for their information and information systems.

The FDIC's Board of Directors has ultimate responsibility for the security of the FDIC's information and information systems. FDIC division and office heads also play an important role in information security. These individuals are responsible for ensuring that information systems under their ownership or control conform to the FDIC's information security program requirements. Further, the FDIC's Chief Information Officer (CIO), who reports directly to the FDIC Chairman, has broad strategic responsibility for information technology (IT) governance, investments, program management, and information security. The FDIC's Chief Information Security Officer

[2] Because the report contained sensitive information, we did not make it available to the public in its entirety. We did, however, post an executive summary of the report on our public Web site at www.fdicig.gov.

(CISO), who reports directly to the CIO, is responsible for carrying out the CIO's responsibilities under FISMA—most notably to plan, develop, and implement an agency-wide information security program. The CIO and CISO coordinate closely with the Director, Division of Information Technology (DIT), who is responsible for managing the FDIC's IT functions. The Director, DIT, reports to the CIO.

Information security managers (ISM) located within the divisions and offices provide a business focus on information security and coordinate with the CIO Organization to ensure that appropriate security controls are in place to protect their respective division or office's information and information systems. ISMs are responsible for such things as educating employees and contractors on how to properly safeguard FDIC information; assessing system security levels; ensuring that security requirements are addressed in new and enhanced systems; and promoting compliance with security policies and procedures. Internal control liaisons within the divisions and offices work with the ISMs to identify and ensure the implementation of appropriate security controls within business processes.

Finally, the Division of Administration's (DOA) Security and Emergency Preparedness Section (SEPS) is responsible for administering the FDIC's physical and personnel security programs, which are fundamental components of the overall information security program. Physical security includes such activities as badging employees, contractors, and visitors and protecting employees, visitors, and facilities from internal and external threats, such as fire, theft, vandalism, sabotage, and terrorist activities. Personnel security includes activities such as performing background investigations and credit checks of FDIC employees and contractor personnel to ensure that the Corporation employs and retains only those persons who meet federal requirements for suitability and whose conduct would not jeopardize the accomplishment of the Corporation's duties or responsibilities.

The Sensitive Nature of Resolution Plans

Section 165(d) of the Dodd-Frank Act requires certain financial companies designated as systemically important to report to the FDIC on their plans for a rapid and orderly resolution under the Bankruptcy Code (title 11 of the United States Code (U.S.C.)) in the event of material financial distress or failure. To implement the requirements of section 165(d), the FDIC and the Board of Governors of the Federal Reserve System (FRB) jointly issued a Final Rule, entitled *Resolution Plans Required*, dated November 1, 2011. The Final Rule requires financial companies covered by the statute to submit resolution plans, sometimes referred to as "living wills," to the FDIC and FRB for review. The intent of this requirement is for a financial company to describe how it could be resolved under the Bankruptcy Code without serious adverse effects on U.S. financial stability.

Within the FDIC, OCFI and the Division of Risk Management Supervision (RMS) have primary responsibility for managing employee access to resolution plans submitted by SIFIs. Resolution plans consist of several components, including an Executive Summary, a narrative description of the SIFI's resolution strategy, supporting appendices, and other information required by the Final Rule. According to OCFI's policy memorandum,

entitled *OCFI Title 1 Security Practices for Review of Resolution Plans Submitted to OCFI under the §165(d) Rule or under the IDI Rule*, dated June 2013, all electronic copies of resolution plans are to be maintained in OCFI Documentum (ODM), Microsoft SharePoint®, or "any other such secure platform or site." ODM serves as the official system of record for electronic copies of the plans. The OCFI policy memorandum also permits FDIC employees with authorized access to resolution plans to print those plans.

The resolution plans required by the Dodd-Frank Act contain some of the most sensitive information that the FDIC maintains. Although not considered to be classified information, the plans can include: information about the critical vendors, suppliers, and associated agreements that SIFIs maintain; a description of the actions that SIFIs would or would not take to support clients and vendors under stress; non-public financial and business data; personal information about employees; the location and activities of data centers; and a list of critical operations. Accordingly, the plans can be an attractive target for persons wishing to steal the information for personal gain, competitive advantage, or to inflict harm upon the Corporation or SIFIs by disseminating the information to criminals, foreign intelligence services, or to the general public.

Individuals that organizations entrust with access to highly sensitive information, such as the resolution plans required by the Dodd-Frank Act, can pose specific types of security risks to organizations. For example, when these "trusted insiders" become disgruntled, they may feel justified in pursuing malicious activity against the organization. Motivations for malicious activity can include politics, morality, anger, revenge, or greed. Because trusted insiders often have knowledge that outside adversaries do not possess, such as an awareness of the organization's vulnerabilities, the associated risk is elevated. Trusted insiders can also inflict harm on an organization through acts of negligence or complacency, such as failing to follow security policies or thwart social engineering efforts, including fraudulent emails (i.e., phishing). These particular types of insider threats have become increasingly common and have been the source of several recent and highly-publicized data breaches across the public and private sectors. Accordingly, special consideration must be given to the risks posed by trusted insiders and appropriate security controls established to mitigate those risks.

The Security Incident Involving Resolution Plans

On September 29, 2015, Information Security and Privacy Staff (ISPS) personnel operating the FDIC's Data Loss Prevention (DLP) tool detected that an employee who had previously worked for OCFI had copied sensitive components of three resolution plans from the network onto an unencrypted Universal Serial Bus (USB) storage device.[3] This activity violated OCFI policy which expressly prohibits the storage of resolution plans on removable media.[4] In addition, the activity appeared suspicious because the

[3] Based on the activity detected by the DLP tool, the employee copied the Executive Summary and the narrative description of the SIFI's resolution strategy for each of the three plans, but did not copy the supporting appendices or documents containing other information required by the Final Rule.
[4] OCFI's policy memorandum, entitled *OCFI Title 1 Security Practices for Review of Resolution Plans Submitted to OCFI under the §165(d) Rule or under the IDI Rule.*

resolution plan information was copied to the USB device immediately prior to the employee's departure. Further, the employee did not have authorization to take any sensitive FDIC information, including resolution plans, upon departure.

Law enforcement officials subsequently recovered the USB device containing the components of the resolution plans copied by the employee. In the course of doing so, these officials also identified and recovered from the employee a sensitive Executive Summary for a fourth resolution plan that was in hard copy. In early October 2015, OCFI officials coordinated with RMS to notify each of the SIFIs impacted by the incident. In addition, law enforcement officials learned that the employee had interviewed for employment with two of the four SIFIs impacted by the incident following the employee's resignation, suggesting that the employee may have taken the resolution plans for personal gain. Further, there were indications prior to the incident that the employee presented a heightened security risk and may not have been suited to have access to highly sensitive information, such as resolution plans.

The security incident involving resolution plans is not an isolated instance of unauthorized exfiltration of sensitive FDIC information by trusted insiders leaving the Corporation. Between February and May 2016, the FDIC notified the Congress of seven major incidents in which employees took significant quantities of sensitive information from the FDIC without authorization when they departed. Such incidents underscore the criticality of establishing and implementing a strong, enterprise-wide information security program that addresses threats that come from both internal and external sources.

Audit Results

We identified a number of factors that contributed to the security incident involving sensitive resolution plans. Most notably, an insider threat program would have better enabled the FDIC to deter, detect, and mitigate the risks posed by the employee. In addition, a key security control designed to prevent employees with access to sensitive resolution plans from copying electronic information to removable media failed to operate as intended. The remaining factors involved OCFI employees having access to resolution plans that exceeded business needs; OCFI's inability to effectively review and revoke employee access to resolution plans because employees were allowed to store copies of the plans outside of ODM; and OCFI's inability to monitor all downloading of resolution plans stored in ODM.

With respect to insider threats, the FDIC has a number of long-standing controls designed to mitigate risks associated with trusted insiders. Such controls include, for example, background investigations, periodic inspections of FDIC facilities to identify security concerns, employee non-disclosure agreements, a Data Loss Prevention tool, and programs to help employees cope with personal issues. During 2014 and 2015, the FDIC began to take steps towards establishing a formal insider threat program by, among other things, developing a proposed governance structure and drafting program policies.

However, these activities were not completed or approved, and progress toward establishing an insider threat program stalled in the fall of 2015.

Following the incident involving resolution plans, OCFI officials assessed the associated risks and began implementing new or enhanced security controls over resolution plans. Such controls included better aligning employee access to resolution plans in ODM with business needs; increasing the frequency of access reviews for plans stored in ODM; and reviewing employee printing activities to identify and investigate suspicious activity. However, because OCFI had not yet developed written policies, procedures, and assessment plans to govern these new or enhanced controls, we did not have criteria against which to test their effectiveness.

Our report describes additional control improvements that the FDIC should implement to better safeguard sensitive resolution plans. It is important to note that no matter how well designed, implemented, or operated, an internal control system cannot provide absolute assurance that all of management's objectives will be met. Factors outside of management's control, such as a trusted insider who is intent on circumventing internal controls, can affect management's ability to achieve its objectives. Accordingly, the control measures we are recommending are intended to help the FDIC achieve reasonable, not absolute, assurance that sensitive resolution plans are adequately safeguarded.

Factors that Contributed to the Incident

An Insider Threat Program Would Have Better Enabled the FDIC to Deter, Detect, and Mitigate the Risks Posed by the Employee

In November 2012, the President issued *Presidential Memorandum—National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, to provide direction and guidance to federal departments and agencies in developing effective insider threat programs to deter, detect, and mitigate actions by employees who may represent a threat to national security. The memorandum requires departments and agencies with access to classified information, or that operate or access classified computer networks, to

> The Presidential Memorandum defines the term "insider threat" as the threat that an insider will use his or her authorized access, wittingly or unwittingly, to harm the security of the United States.
>
> Risks posed by trusted insiders include such things as the theft of confidential or business proprietary information, IT sabotage, fraud, and threats against agency assets or personnel.

implement an insider threat program.[5] The FDIC has access to a limited amount of classified information. The insider threat program described in the Presidential Memorandum should employ risk management principles that are tailored to meet the distinct needs, mission, and systems of individual agencies and include appropriate protections for privacy, civil rights, and civil liberties.

In April 2013, NIST issued SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The publication states that the standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of unclassified information in non-national security systems. SP 800-53 identifies a number of critical elements associated with insider threat programs, including:

- a senior organizational official who is designated by the department/agency head as being responsible for implementing and providing oversight of the program;
- formal policies and implementation plans that address roles, responsibilities, and associated program activities;
- host-based user monitoring of employee activities on government-owned classified computers;
- a cross-discipline team and security controls aimed at detecting and preventing malicious insider activity through the centralized integration and analysis of both technical and non-technical information;
- employee awareness training of insider threats and employees' reporting responsibilities;
- self-assessments of compliance with insider threat policies and standards and the department/agency's insider threat posture; and
- participation of a legal team to ensure that monitoring activities are performed in accordance with appropriate laws, directives, regulations, policies, standards, and guidelines.

NIST SP 800-53 states that it is important for the cross-discipline team focused on insider threats to have access to information from all relevant offices (e.g., human resources, legal, physical security, personnel security, IT, information system security, and law enforcement).[6] Human resource records are especially important to insider threat

[5] Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, which was issued in October 2011, also requires agencies that handle classified information to establish insider threat programs. Both Executive Order 13587 and the November 2012 Presidential Memorandum are legally applicable to the FDIC.

[6] Information from an organization's counterintelligence function (if one exists) can also benefit the cross-discipline team.

analysis as there is compelling evidence to demonstrate that some types of insider crimes are often preceded by behaviors that do not involve technology, such as ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues. This information, along with the results of background investigations from personnel security offices, can better focus insider threat management efforts.

Risks Posed by the Employee and the FDIC's Response

In the years leading up to the incident, there were indications that the employee involved in the incident posed a heightened security risk and may not have been suited to work with highly sensitive corporate information, such as resolution plans. Most significantly, we noted:

- **Personal Financial Issues.** A background investigation of the employee conducted upon initial employment at the FDIC identified major financial problems that raise serious questions about the employee's suitability to work for the FDIC and handle sensitive information.[7]

- **Signs of Disgruntlement.** Corporate human resource records indicate that the employee was involved in several disputes with FDIC management and repeatedly expressed dissatisfaction with management's decision-making and treatment of the employee.

- **Performance Concerns.** The employee's performance management records indicate that the employee repeatedly demonstrated poor judgment, a lack of accountability for actions, and an inability to follow supervisor instructions or acknowledge and adhere to FDIC policies. For example, the employee violated FDIC security policy several months prior to the incident by transmitting unencrypted, sensitive information to two personal email accounts and subsequently refused to acknowledge that this activity was prohibited.

We spoke with officials in OCFI, DOA's Labor and Employee Relations Section, and the Legal Division's Labor, Employment, and Administration Section about the risks associated with the employee. These officials informed us that they had coordinated to take various disciplinary and performance-based actions against the employee in the period leading up to the employee's resignation. Such actions included:

- issuing a letter of warning to the employee in January 2015 in response to numerous performance and behavioral deficiencies since September 2013;

[7] Our audit did not include an assessment of the FDIC's adjudication of the employee's background investigation. The OIG issued a separate evaluation report in August 2014, entitled *The FDIC's Personnel Security and Suitability Program* (Report No. EVAL-14-003), that reviewed (among other things) adjudications. The report stated that most preliminary clearance and adjudication determinations reviewed during the evaluation were completed appropriately. However, the report questioned a number of determinations and found that some determinations lacked support. The report can be found at www.fdicig.gov.

- placing the employee on a formal performance improvement plan (PIP) in June 2015 because the employee did not address the above referenced deficiencies;

- suspending the employee for 5 days without pay in July 2015 for various types of misconduct; and

- informing the employee in August 2015 that the employee's performance and behavior had not improved during the course of the PIP.

More severe action, such as terminating the employee, became unnecessary when the employee resigned in September 2015.

We noted that the employee retained access to view, download, and print sensitive resolution plans stored in ODM for all SIFIs until the employee's last day of employment. The FDIC officials that we spoke with indicated that taking additional risk mitigation actions, such as limiting or restricting the employee's access to sensitive information or subjecting the employee to increased monitoring, could have exposed the FDIC to potential legal risk, such as a claim that the employee was receiving disparate treatment.

An insider threat program would have better enabled the FDIC to address the risks associated with the employee. For example, OCFI officials were not aware that the employee's background investigation had identified significant financial problems when they granted the employee access to resolution plans. DOA typically does not provide the FDIC's business units with such information due to privacy concerns. Instead, business units only receive an indication of whether the employee's background investigation was favorably or unfavorably adjudicated. A cross-discipline team with access to employee personnel information and operating under an insider threat program would likely have informed OCFI management of the risks associated with the employee's financial problems, potentially resulting in a management decision to not grant the employee access to any resolution plans. Further, an insider threat program could have allowed for increased monitoring of the employee through a formalized process less susceptible to claims of unfair targeting or retaliation.

Efforts to Establish an Insider Threat Program at the FDIC

The FDIC has a number of long-standing security controls designed to mitigate risks associated with trusted insiders. These controls include such things as background investigations, periodic inspections of FDIC facilities to identify security concerns, employee non-disclosure agreements, the DLP tool, and programs to help employees cope with personal issues. More recently, the FDIC began to take steps towards establishing a formal insider threat program. In May 2014, SEPS engaged a consultant to conduct a study of how counterintelligence could be incorporated into the FDIC's security programs. The study resulted in 10 recommendations that were presented to senior FDIC management in August 2014. In response to one of the study's

recommendations, SEPS hired a Counterintelligence Officer in January 2015 to establish a counterintelligence capability and help "manage insider threats, data loss, and other similar situations."

In April 2015, the focus of the FDIC's efforts to build a counterintelligence capability shifted toward establishing a corporate-wide Internal Protection Program (IPP) aimed at addressing threats and risks posed to FDIC personnel, facilities, resources, and information by foreign entities or insider threats. Accordingly, an insider threat program was to be a critical component of the IPP. Between April and August 2015, the FDIC drafted a governance charter and policy for the IPP and drafted a policy for the insider threat program. However, these documents were never completed or approved. The FDIC's Counterintelligence Officer accepted a position with another agency in August 2015, and progress toward developing the IPP and insider threat program stalled. At the close of our audit, the Counterintelligence Officer position remained vacant. On March 22, 2016, SEPS officials briefed the FDIC's Executive Management Committee (EMC)[8] on the status of efforts to establish the IPP and insider threat program.

Although the FDIC has taken steps towards establishing an insider threat program, priority attention needs to be placed on completing and approving a formal governance structure, policies, procedures, and plans, as well as hiring key personnel, to manage and implement the program. Once implemented, an insider threat program will better position the FDIC to deter, detect, and respond to risks posed by trusted insiders, such as the employee involved in the resolution plans incident. Because the establishment and implementation of an insider threat program will require the coordination of divisions and offices throughout the FDIC, the EMC is in a position to facilitate such an effort.

Recommendation

We recommend that the Deputy to the Chairman, Chief Operating Officer, and Chief of Staff:

1. Coordinate with the EMC to establish a corporate-wide insider threat program that is consistent with NIST-recommended practices and applicable laws, Executive Orders, national strategies, directives, regulations, policies, standards, and guidelines.

A Key Control Intended to Prevent the Copying of Sensitive Resolution Plans to Removable Media Did Not Function Properly

NIST SP 800-53 states that organizations can physically disable or remove USB ports to help prevent the exfiltration of information from information systems. In this regard,

[8] The FDIC Chairman established the EMC in 2012 to assist the Chairman and Board of Directors in the day-to-day operational and strategic management of the FDIC. The Deputy to the Chairman, Chief Operating Officer, and Chief of Staff serves as the EMC's Chairman. The EMC is responsible for identifying key operational and strategic priorities and overseeing the timely coordination of issue follow-up.

OCFI worked in coordination with DIT to establish an IT control in 2013 to restrict employees with access to resolution plans from copying electronic information from the internal network to removable media.[9] Implementation of the control involved adding the Network IDs of employees to a Microsoft Windows Active Directory® (AD) User Group that blocked the employees from using removable media.

This control did not function properly as the employee involved in the incident was able to copy sensitive components of resolution plans to removable media, placing the operations and reputation of the FDIC and the affected SIFIs at significant risk. During our audit, DIT officials conducted an analysis of the circumstances and events pertaining to the incident in an attempt to identify the cause of the control breakdown. According to the DIT officials, FDIC computer security records indicate that the employee was added to the AD User Group in November 2013. However, DIT officials also determined that the version of a security software program running on the employee's computer that interacted with the AD User Group had a vulnerability that would allow a user, under certain circumstances, to copy data to removable media. DIT officials concluded that these circumstances may have occurred in the case of the employee. At the close of our audit, DIT was working to eliminate the vulnerability by upgrading the software program to a more current version.

At the time of the incident, OCFI and the CIO Organization had not coordinated to establish policies, procedures, or assessment plans to ensure the control was repeatable, consistent, and disciplined; operating as intended; and producing the desired outcomes with respect to meeting OCFI's security requirements. A contributing factor for the lack of policies, procedures, or assessment plans may have been the departure of OCFI's permanent ISM in April 2014. Since then, an ISM from another FDIC division has been serving as OCFI's ISM on a part-time basis. A dedicated ISM would provide OCFI greater assurance that security requirements are being fully addressed and would be consistent with FDIC Circular 1310.3, *Information Security Risk Management Program.* The circular was revised in March 2015 to (among other things) place greater emphasis on the responsibilities of divisions and offices to ensure that security risks and controls are addressed throughout the life cycle of their information systems. ISMs play a critical role in fulfilling such responsibilities as they are often in the best position to identify and address security risks that are specific to the business processes and controls within their divisions and offices.[10]

Written policies and procedures are an important control for reducing operational risk associated with changes in staff, such as the departure of OCFI's ISM in April 2014. The

[9] This control was one of seven controls that we determined to be particularly relevant at the time of the incident. Our review of the remaining six controls found that they were implemented for the employee. See Appendix 1 for a description of the seven controls we reviewed.

[10] In our audit report entitled, *Audit of the FDIC's Information Security Program—2015* (Report No. AUD-16-001, dated October 28, 2015), we recommended that the FDIC assess the role of the ISMs in managing information security risks within the FDIC's divisions and offices—including an analysis of the resources needed to ensure ISM duties are successfully executed—and establish a plan to address any identified gaps. As of the date of this report, these recommendations remain open.

Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* state that policies and procedures are an integral part of an organization's operations and a key control for ensuring that management's directives are carried out. In addition, the NIST Risk Management Framework in SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, identifies security control documentation as a key component of effectively managing information security risk. Finally, Circular 4010.3, *FDIC Enterprise Risk Management Program*, requires divisions and offices to maintain current policies and procedures. Periodically assessing the effectiveness of controls is also consistent with GAO's *Standards for Internal Control in the Federal Government* and Circular 4010.3.

In recognition of the growing risks associated with removable media, the FDIC Chairman notified all employees and contractor personnel via email that, effective March 18, 2016, they were no longer permitted to copy data to removable media except in cases approved by an FDIC division or office director. In addition, the FDIC began to change underlying business processes to eliminate the need for removable media (to the extent practical) for those processes that require the use of removable media. As of June 28, 2016, DIT officials reported that 1,089 of 16,922 (or 6 percent) network accounts had permission to copy information to removable media. In our view, this presents a continued risk to the Corporation. To help mitigate this risk, DIT was working to issue a software release at the close of our audit that would require information copied to USB devices to be encrypted. This new requirement is intended to protect sensitive information stored on removable media should the media become lost or stolen. DIT is also working to establish a procedure for granting exceptions for staff that need the ability to save unencrypted information to removable media.

Recommendations

We recommend that the CIO:

2. Immediately test the effectiveness of the control designed to prohibit network users from copying information to removable media to confirm that the control operates as intended.

3. Coordinate with division and office directors to revise and/or develop written policies and procedures, as appropriate, to govern the control designed to prohibit network users from copying information to removable media. Such policies and procedures should address the prohibitions contained in the Chairman's March 2016 email, protocols for managing exceptions, and requirements for regular testing of the control's effectiveness.

We recommend that the Director, OCFI:

4. Assign a dedicated information security manager to support OCFI.

Employee Access to Resolution Plans Should Have Been More Consistent with Business Needs

FDIC Circular 1360.15, *Access Control for Information Technology Resources,* requires that the security principle of least privilege be applied to user access to information and systems. Least privilege refers to the practice of restricting user access (to data files, to processing capability, or to peripherals) or type of access (i.e., read, write, execute, or delete) to the minimum necessary to perform the user's job. At the time of the incident, employees with authorization to access sensitive resolution plans had the ability to view, download, and print plans stored in ODM for all SIFIs, unless the employee had identified a conflict on their OCFI *Conflict of Interest Statement*. The employee involved in the incident had authorization to access these resolution plans and had not identified any such conflicts.

Subsequent to the incident, OCFI began implementing a control to place greater restrictions on employee access to resolution plans stored in ODM based on the employee's specific assignments. As discussed later, OCFI needed to develop written policies and procedures that address new and enhanced controls established subsequent to the incident, including the increased restrictions on employee access to resolution plans. Because we address this issue in the following section of this report, we are not making a recommendation with respect to employee access to resolution plans.

OCFI Was Not Able to Effectively Review and Revoke Access to Resolution Plans

FDIC Circular 1360.15 requires that user access privileges to information and systems be periodically reviewed to ensure they remain consistent with business needs and revoked when access is no longer required. While OCFI had established processes for reviewing and revoking access privileges to resolution plans stored in ODM, OCFI policy also allowed employees to store copies of plans in Microsoft SharePoint® or "any other such secure platform or site." Further, OCFI policy allowed employees with access to resolution plans to print those plans. As a result, employees had the ability to store numerous copies of plans on the internal network and inside their physical work spaces, impairing OCFI's ability to effectively review access privileges to resolution plans to ensure they remained consistent with business needs and revoke access when it was no longer needed.

Recommendation

We recommend that the Director, OCFI:

5. Evaluate whether employees should continue to be allowed to store copies of sensitive resolution plans outside of ODM, and if so, determine what additional mitigation strategies may be warranted to address the associated risk.

OCFI Was Not Able to Monitor All Downloading of Resolution Plans

NIST SP 800-53 recommends that agencies periodically review and analyze information system logs for indications of inappropriate or unusual activity and report findings to appropriate personnel. ODM was designed to log the downloading of sensitive resolution plan components when the downloading is initiated using menu options offered within ODM. However, ODM did not log these downloads when they were initiated using menu options within the default applications used to store the files (e.g., Microsoft Word® for documents, Microsoft Excel® for spreadsheets, and Adobe Acrobat® for PDF files). Once downloaded, ODM users can make electronic copies of, or print, resolution plans.[11]

OCFI should consider whether all downloading of resolution plans from ODM can and should be logged and monitored. Such consideration should be made when addressing Recommendation 5 in this report.

OCFI Has Begun Implementing Several Mitigating Controls, but Work Remains to Establish Policies and Procedures to Govern the Controls

Following the incident involving resolution plans, OCFI officials assessed the risks associated with the incident and began implementing new or enhanced security controls over resolution plans based on the results of the assessment. Such controls included:

- limiting the ability of employees to view, download, and print resolution plans stored in ODM to a subset of SIFIs based on the specific job duties of the employee;
- increasing the frequency of reviews of employee access to resolution plans in ODM from bi-monthly to monthly to ensure access privileges remain consistent with business needs;
- coordinating with ISPS to expand the parameters used to block email communications addressed to non-FDIC email accounts that appear to contain content related to resolution plans;
- conducting weekly reviews of print activity by ODM users with access to sensitive resolution plans to identify and investigate suspicious activity (e.g., large print jobs); and

[11] As noted in the following section of this report, OCFI has begun to monitor print activity for ODM users with access to resolution plans.

- conducting bi-weekly comparisons of recently separated or transferred employees to ODM users with access to resolution plans to help ensure that access is promptly disabled, when appropriate.

OCFI had not yet developed written policies, procedures, and assessment plans to govern the controls described above. Accordingly, we did not have criteria against which to test the effectiveness of these controls. However, we did review documentation confirming that OCFI had begun implementing each of these controls. OCFI officials indicated that they intend to develop policies, procedures, and assessment plans in the near future to ensure that the new and enhanced controls are repeatable, consistent, and disciplined; operating as intended; and producing the desired outcomes with respect to meeting OCFI's security requirements. Doing so would be consistent with GAO standards, FDIC policy, and NIST guidance.

Recommendation

We recommend that the Director, OCFI:

6. Develop appropriate policies and procedures that address the new and enhanced security controls established by OCFI subsequent to the incident and establish and implement plans to periodically assess the effectiveness of those controls.

Corporation Comments and OIG Evaluation

The Deputy to the Chairman, Chief Operating Officer, and Chief of Staff; the CIO; and the Director, OCFI; provided a joint written response, dated June 28, 2016, to a draft of this report. The response is provided in its entirety in Appendix 4. In the response, FDIC management concurred with all six of the report's recommendations. A summary of the Corporation's corrective actions is presented in Appendix 5. The planned actions are responsive to the recommendations and the recommendations are resolved.

Appendix 1

Objectives, Scope, and Methodology

Objectives

The objectives of the audit were to (a) determine the factors that contributed to the security incident involving sensitive resolution plans and (b) assess the adequacy of mitigating controls established subsequent to the incident.

We performed audit fieldwork from February through May 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope and Methodology

To determine the factors that contributed to the incident, we first interviewed officials in OCFI, DOA, RMS, ISPS, DIT, and the Legal Division to obtain an understanding of the facts and circumstances surrounding the incident and the security controls that should have been implemented for the employee at that time. Next, based on the results of these interviews and our review of relevant policies, procedures, guidelines, and records, we identified the following seven controls established by FDIC management at the time of the incident that we determined to be particularly relevant.

1. The employee should have received a favorable determination from DOA on a high-risk background investigation within the last 5 year(s), or been the subject of an ongoing, initial high-risk background investigation.

2. The employee should have completed an OCFI *Acknowledgement of Confidentiality Obligations* within 2 years of departure.

3. The employee should have affirmed the responsibilities agreement at the end of the FDIC's online Information Security and Privacy Awareness Training within 1 year of departure.

4. The employee should have been technically restricted from copying electronic information, including sensitive resolution plans, from the FDIC network to removable media.

5. The employee should have been subject to the FDIC's performance management program.

6. The employee should have been subjected to possible disciplinary action for violating an FDIC information security policy in April 2015.

Objectives, Scope, and Methodology

7. The employee should have certified when completing the Corporation's pre-exit clearance procedures that no sensitive information related to financial institutions would be taken from the FDIC upon departure.[12]

We then assessed whether each of these controls was implemented for the employee by examining records related to the incident and evidence of control implementation, such as personnel files and training records. In addition to the failure of control number 4 listed above for the employee, we identified control gaps (i.e., unestablished controls) that, taken together, we considered to be the principal factors that contributed to the incident.

To assess the adequacy of mitigating controls established subsequent to the incident, we interviewed OCFI and DIT officials to learn about new or enhanced security controls and considered the extent to which these controls addressed the factors that contributed to the incident. We also reviewed documentation to determine whether implementation of each of these controls had begun. However, because OCFI had not yet developed written policies, procedures, and assessment plans to govern these controls, we did not have criteria against which to test the effectiveness of the controls. Accordingly, we did not perform such tests.

The primary criteria used in the audit was as follows:

- Section 112(d)(5) of the Dodd-Frank Act (12 U.S.C. § 5322), which states that members of the Financial Stability Oversight Council, including the FDIC, ''shall maintain the confidentiality of any data, information, and reports submitted under'' title I of the statute (which includes section 165(d)).

- The Final Rule, entitled *Resolution Plans Required*, which states that institutions that file resolution plans are to indicate to the regulators which portions of the plans are confidential and which portions can be made public.

- FISMA, which requires federal agencies, including the FDIC, to (a) develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency and (b) provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, or disclosure of information collected or maintained by the agency.

- Security guidelines issued by NIST that assist agencies in defining security requirements for their information systems.

[12] Completion of the pre-exit clearance procedures is designed to help safeguard FDIC-owned property and interests when employees leave the Corporation. We did not audit the completion of the pre-exit clearance procedures in their totality.

Appendix 1

Objectives, Scope, and Methodology

- GAO's *Standards for Internal Control in the Federal Government*, dated September 2014, that defines an overall framework for establishing and maintaining effective internal controls in federal agencies.

- Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, which requires agencies that handle classified information to establish insider threat programs.

- *Presidential Memorandum—National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, which provides direction and guidance to federal departments and agencies in developing effective insider threat programs. The memorandum requires departments and agencies with access to classified information, or that operate or access classified computer networks, to implement an insider threat program.

- FDIC information security policies, procedures, and guidelines designed to protect sensitive information from unauthorized disclosure. A key policy with respect to safeguarding resolution plans is OCFI's memorandum, entitled *OCFI Title 1 Security Practices for Review of Resolution Plans Submitted to OCFI under the §165(d) Rule or under the IDI Rule*, dated June 2013.

In planning this audit, we considered the results, conclusions, and recommendations pertaining to our audit report, entitled *The FDIC's Controls for Safeguarding Sensitive Information in Resolution Plans Submitted Under the Dodd-Frank Act* (Report No. AUD-14-008, dated July 3, 2014).

We performed our audit work at the FDIC's offices in Arlington, Virginia, and Washington, D.C.

Appendix 2

Glossary of Terms

Term	Definition
Confidential Information	Within the context of the Dodd-Frank Act, the terms confidential and confidentiality have been defined by the Final Rule to mean not releasing information from the resolution plans that the submitter considers confidential and not releasable to the public under the Freedom of Information Act (5 U.S.C. § 552) or FRB and/or FDIC regulations (12 Code of Federal Regulations (C.F.R.) parts 261 and 309). Under FISMA (Public Law (P.L.) No. 113-283), the terms confidential and confidentiality are defined as preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information.
Conflict of Interest Statement	In the context of this report, a Conflict of Interest Statement is completed by an FDIC employee to identify any conflicts of interest with respect to SIFIs prior to obtaining access to sensitive resolution plans so that only appropriate access will be granted.
Counterintelligence	Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.
Data Loss Prevention	Sometimes referred to as data leak prevention or information loss prevention, the term refers to a strategy for mitigating the risk of end users transmitting sensitive information outside of the organization. In the context of this report, the term refers to a software tool designed to detect and, if enabled, prevent potential data breaches by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
Major Incident	An information security incident that meets the criteria defined in the Office of Management and Budget's Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*. FISMA requires federal agencies to notify and consult with, as appropriate, the Congressional Committees referenced in the statute for major incidents. According to FISMA, Congressional notification and consulting is to occur not later than 7 days after the date on which there is a reasonable basis to conclude that a major incident has occurred.
Microsoft Windows Active Directory®	An IT service in the Windows Server® operating system platform that is used to centrally manage user accounts and security settings (including access).
Phishing	A digital form of social engineering that uses authentic looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information.

Appendix 2

Glossary of Terms

Term	Definition
Resolution Plans	Section 165(d) of the Dodd-Frank Act requires each bank holding company with total consolidated assets of $50 billion or more and each nonbank financial company designated by the Financial Stability Oversight Council (FSOC) for enhanced supervision by the FRB to report periodically to the FDIC, FRB, and FSOC on the plan of such company for its rapid and orderly resolution in the event of material financial distress or failure. To implement this requirement, the FDIC and FRB jointly issued a Final Rule, entitled *Resolution Plans Required*, on November 1, 2011, that requires financial companies covered by the statute to submit resolution plans describing the company's strategy for a rapid and orderly resolution under the Bankruptcy Code in the event of material financial distress or failure of the company.
Social Engineering	In the context of information security, social engineering refers to the psychological manipulation of people causing them to perform actions or divulging confidential information.
Sensitive Information	In general, sensitive information is information that contains an element of confidentiality. It includes information that is exempt from disclosure by the Freedom of Information Act and information whose disclosure is governed by the Privacy Act of 1974 (5 U.S.C. § 552a). Sensitive information requires a high level of protection from loss, misuse, and unauthorized access or modification.
Systemically Important Financial Institution	Refers to bank holding companies with $50 billion or more in total consolidated assets and nonbank financial companies designated by the FSOC for FRB supervision and enhanced prudential standards of the Dodd-Frank Act (12 U.S.C. §§ 5322 and 5323).

Appendix 3

Abbreviations and Acronyms

Abbreviation/Acronym	Explanation
AD	Microsoft Windows Active Directory®
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DIT	Division of Information Technology
DLP	Data Loss Prevention
DOA	Division of Administration
EMC	Executive Management Committee
FISMA	Federal Information Security Modernization Act of 2014
FRB	Board of Governors of the Federal Reserve System
FSOC	Financial Stability Oversight Council
GAO	Government Accountability Office
IPP	Internal Protection Program
ISM	Information Security Manager
ISPS	Information Security and Privacy Staff
NIST	National Institute of Standards and Technology
OCFI	Office of Complex Financial Institutions
ODM	OCFI Documentum
OIG	Office of Inspector General
PIP	Performance Improvement Plan
RMS	Division of Risk Management Supervision
SEPS	Security and Emergency Preparedness Section
SIFI	Systemically Important Financial Institution
SP	Special Publication
USB	Universal Serial Bus
U.S.C.	United States Code

Appendix 4

Corporation Comments

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C., 20429

DATE: June 28, 2016

MEMORANDUM TO: Mark F. Mulholland
Assistant Inspector General for Audits

FROM: Barbara A. Ryan /Signed/
Deputy to the Chairman and Chief Operating Officer/Chief of Staff

Arthur J. Murton, Director /Signed/
Office of Complex Financial Institutions

Lawrence Gross /Signed/
Chief Information Officer

SUBJECT: Management Response to the Draft OIG Audit Report Entitled *The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans* (Assignment No. 2016-018)

The Federal Deposit Insurance Corporation (FDIC) has completed its review of the Office of Inspector General's (OIG) draft audit report entitled *The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans Submitted Under the Dodd-Frank Act* (Assignment No. 2016-018), dated June 8, 2016.

We appreciate the OIG's analysis and findings regarding the FDIC's controls for safeguarding resolution plans. We recognize the need to improve those controls and address identified weaknesses. The draft report notes that the FDIC has recently implemented a number of controls designed to mitigate the information security risks associated with sensitive resolution plans. It also acknowledges that the FDIC has a number of long-standing controls designed to mitigate risks associated with trusted insiders. However, the report identifies six recommendations for improvements to strengthen information security and FDIC management concurs with these recommendations. We are committed to addressing each of the recommendations to further strengthen our controls and lower the risk of harm from the unauthorized release of sensitive information.

Our detailed response below is organized by recommendation and contains actions planned or in process and those that have been completed.

Recommendation 1: The OIG recommends that the Deputy to the Chairman and Chief Operating Officer/Chief of Staff (COO/COS) coordinate with the Executive Management Committee (EMC) to establish a corporate-wide insider threat program that is consistent with NIST-recommended practices and applicable laws, Executive Orders, national strategies, directives, regulations, policies, standards, and guidelines.

Appendix 4

Corporation Comments

Management Decision: Concur

Corrective Actions: As noted by the OIG, with respect to insider threats, the FDIC has a number of long-standing controls designed to mitigate risks associated with trusted insiders, including background investigations, periodic inspections of FDIC facilities to identify security concerns, employee non-disclosure agreements, a Data Loss Prevention (DLP) tool, and programs to help employees with personal issues.

In 2014 and 2015, the FDIC began to take steps toward establishing a formal insider threat program by developing draft governance, policy, and procedures documents, and by initiating interdivisional discussions on the topic. However, as of October 2015, the insider threat program had not been implemented. As noted by the OIG, such a program would have better enabled the FDIC to deter, detect, and mitigate the risks posed by the employee.

The COO/COS, with the EMC, has engaged a cross-disciplinary team composed of FDIC executive-level staff from the human resources, legal, physical security, and information system areas to formally establish a corporate-wide insider threat program consistent with NIST-recommended practices and applicable laws, Executive Orders, national strategies, directives, regulations, policies, standards, and guidelines. This team is finalizing the FDIC's insider threat program policy statement and governance structure. The FDIC is committed to completing this by October 28, 2016.

A key component of the formal insider threat program is the establishment of an insider threat working group composed of key stakeholder groups (including representatives from the Division of Administration/Security, CIO/CISO, Legal Division and other major divisions/offices) and chaired by a senior FDIC official designated as being responsible for implementing and providing oversight of the program. The insider threat working group will focus on identifying, mitigating, and preventing malicious insider threat activity. It will meet on a regular basis and convene ad hoc meetings to address exigent threats or concerns to the FDIC as needed. The FDIC is committed to establishing the insider threat working group by October 28, 2016.

Employee awareness will be critical to the success of the FDIC's insider threat program. Introductory outreach briefings on the program will be conducted in both headquarters and regional offices to ensure employee awareness of the new program and its requirements. The FDIC is committed to conducting information awareness briefings from the date of program implementation through the end of the year and to integrating insider threat program employee awareness training into the existing security training module by December 30, 2016.

Completion Dates: From October 2016 through December 2016 as identified above.

Appendix 4

Corporation Comments

Recommendation 2: The OIG recommends that the CIO immediately test the effectiveness of the control designed to prohibit network users from copying information to removable media to confirm that the control operates as intended.

Management Decision: Concur

Corrective Action: The OIG noted that a key security control designed to prevent employees with access to sensitive resolution plans from copying electronic information to removable media failed to operate as intended. Between October 2015 and April 2016, the Division of Information Technology (DIT) coordinated tests with OCFI and others to ensure the software that prohibits copying files to removable media was working properly. While the majority of the tests were successful, some tests identified defects in limited situations. We are now installing a new software version that addresses the observed defects and plan that installation to be complete by August 26, 2016. Documentation of the test steps and the results of the test will be improved. In addition, DIT will develop a comprehensive test plan and use it to re-evaluate regularly the effectiveness of the software that prohibits users from copying information to removable media.

Completion Date: August 26, 2016

Recommendation 3: The OIG recommends that the CIO coordinate with division and office directors to revise and/or develop written policies and procedures, as appropriate, to govern the control designed to prohibit network users from copying information to removable media. Such policies and procedures should address the prohibitions contained in the Chairman's March 2016 email, protocols for managing exceptions, and requirements for regular testing of the control's effectiveness.

Management Decision: Concur

Corrective Action: The CIO organization will coordinate with division and office directors to identify and update relevant directives and procedures to ensure that they are consistent with the decision to discontinue copying information to removable media. Updated directives and procedures will include protocols for managing any limited exceptions and requirements for regular testing of the control's effectiveness.

Completion Date: September 30, 2016

Recommendation 4: The OIG recommends that the Director, OCFI, assign a dedicated information security manager to support OCFI.

Management Decision: Concur

Appendix 4

Corporation Comments

Corrective Action: OCFI will work with DOA's Human Resources Branch to announce and fill a vacancy for a dedicated information security manager (ISM) position, rather than continuing to share an ISM with the Division of Insurance and Research. A dedicated ISM will ensure that appropriate security controls are in place to better protect OCFI's resolution plan information and information systems.

Completion Date: December 30, 2016

Recommendation 5: The OIG recommends that the Director, OCFI, evaluate whether employees should continue to be allowed to store copies of sensitive resolution plans outside of OCFI Documentum (ODM), and if so, determine what additional mitigation strategies may be warranted to address the associated risk.

Management Decision: Concur

Corrective Action: OCFI is updating its policy regarding the storage of sensitive information. The revised policy will specifically prohibit the practice of storing sensitive resolution plans outside of ODM, including in other secure locations such as hard drives and personal U: drives. It will also address print and download controls. We will continually monitor this policy as the FDIC considers new technologies to store and secure sensitive information.

Completion Date: September 30, 2016

Recommendation 6: The OIG recommends that the Director, OCFI, develop appropriate policies and procedures that address the new and enhanced security controls established by OCFI subsequent to the incident and establish and implement plans to periodically assess the effectiveness of those controls.

Management Decision: Concur

Corrective Action: OCFI is revising its policies and procedures to address the new and enhanced security controls established subsequent to the incident, as described in the OIG's draft report. OCFI will also develop comprehensive procedures that will incorporate control activities to mitigate program risks and ensure that resolution plans are adequately safeguarded. In addition to developing comprehensive policies and procedures, OCFI will conduct internal reviews to periodically test these controls to ensure that the controls are repeatable, consistent, disciplined, and operating as intended.

Completion Date: September 30, 2016

Questions regarding this response should be directed to Rack Campbell at (703) 562-1422.

Appendix 4

Corporation Comments

cc: James H. Angel, Jr., Deputy Director, DOF, Corporate Management Control
Stephen M. Hanas, Legal Division
Titus S. Simmons, Lead Planning and Resource Management Analyst, OCFI, Organizational, Planning & Resource Management
Roderick E. Toms, Acting CISO, Information Security & Privacy
Russell G. Pittman, Director, DIT
Isaac E. Hernandez, Deputy Director, DIT, Infrastructure Services Branch
Steven P. Anderson, Deputy Director, DIT, Business Administration Branch
Rack D. Campbell, Supervisory IT Specialist, DIT, Audit and Internal Control

5

Appendix 5

Summary of the Corporation's Corrective Actions

This table presents corrective actions taken or planned by the Corporation in response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The FDIC will finalize the insider threat program policy statement and governance structure, establish an insider threat working group to implement and oversee the program, and provide awareness briefings to employees on the new program and its requirements.	12/30/2016	$0	Yes	Open
2	DIT will complete the installation of new software that addresses known vulnerabilities in the security control designed to prevent employees from copying sensitive information to removable media. In addition, the CIO Organization will develop a test plan and use it to re-evaluate regularly the effectiveness of the control.	8/26/2016	$0	Yes	Open
3	The FDIC will identify and update relevant directives and procedures to ensure they are consistent with the management decision to discontinue copying information to removable media. Updated directives and procedures will include protocols for managing exceptions and requirements for regular control testing.	9/30/2016	$0	Yes	Open
4	The FDIC will announce and fill a position for a dedicated ISM to support OCFI.	12/30/2016	$0	Yes	Open
5	OCFI will update its policy regarding the storage of sensitive information to prohibit the practice of storing sensitive resolution plans outside of ODM. The update will also address controls over printing and downloading.	9/30/2016	$0	Yes	Open
6	OCFI will revise its policies and procedures to address new and enhanced security controls	9/30/2016	$0	Yes	Open

Appendix 5

Summary of the Corporation's Corrective Actions

	established subsequent to the incident involving sensitive resolution plans and described in this report. In addition, OCFI will develop comprehensive procedures that incorporate control activities to mitigate program risks and ensure that resolution plans are adequately safeguarded. Further, OCFI will conduct internal reviews to periodically test these controls.				

[a] Resolved – (1) Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but alternative action meets the intent of the recommendation.
(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Recommendations will be closed when (a) Corporate Management Control notifies the OIG that corrective actions are complete or (b) in the case of recommendations that the OIG determines to be particularly significant, when the OIG confirms that corrective actions have been completed and are responsive.

Office of Inspector General

Office of Audits and Evaluations
Report No. AUD-16-004

The FDIC's Process for Identifying and Reporting Major Information Security Incidents

July 2016

Office of Inspector General

Executive Summary

The FDIC's Process for Identifying and Reporting Major Information Security Incidents

Report No. AUD-16-004
July 2016

Why We Did The Audit

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program that includes (among other things) procedures for detecting, reporting, and responding to information security incidents. Such procedures are to include notifying and consulting with, as appropriate, the Congressional Committees referenced in the statute for major incidents. According to FISMA, Congressional notification and consulting is to occur not later than 7 days after the date on which there is a reasonable basis to conclude that a major incident has occurred.

FISMA requires the Office of Management and Budget (OMB) to develop guidance on what constitutes a major incident and directs agencies to report incidents designated as major. Accordingly, OMB issued Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 30, 2015, (OMB Memorandum M-16-03) that provides agencies with a definition of the term "major incident" and a framework of factors, the combination of which agencies must consider when characterizing an incident as major. The OMB memorandum states that agencies should notify affected individuals, in accordance with FISMA, as "expeditiously as practical, without unreasonable delay." The memorandum adds that although agencies may consult with the Department of Homeland Security's United States Computer Emergency Readiness Team when determining whether an incident is considered a "major incident," it is ultimately the responsibility of the victim agency to make the determination.

The audit objective was to determine whether the FDIC had established key controls that provide reasonable assurance that major incidents are identified and reported in a timely manner. As part of the audit, we conducted a detailed review of the FDIC's incident investigation-related activities, records, decisions, and reports for one specific incident (referred to herein as the Florida Incident).

Background

Information security incidents at the FDIC can be identified through a variety of sources. For example, employees and contractors must contact the FDIC's Help Desk/Computer Security Incident Response Team (collectively referred to herein as CSIRT) to report a suspected security incident; technologies used by the FDIC to monitor network activity, such as the Data Loss Prevention (DLP) tool, may identify apparent security policy violations; and outside organizations may notify the FDIC of illegal or suspicious activity involving the FDIC's information technology resources.

The FDIC's Information Security and Privacy Staff (ISPS) within the Chief Information Officer (CIO) Organization has overall responsibility for analyzing, reporting, and remediating information security incidents. ISPS reports to the Acting Chief Information Security Officer, who reports to the CIO. The CIO reports to the FDIC Chairman. Other organizational components also play a role in addressing information security incidents. Most notably, CSIRT provides technical assistance and investigates, reports, resolves, and closes incidents by working with FDIC system administrators, division and office Information Security Managers, Privacy Program Office staff, the Data Breach Management Team for data breaches, and others.

Our audit focused on the FDIC's processes for addressing one particular type of information security incident—a breach of sensitive information—because the incident we selected for detailed review (i.e., the Florida Incident) was a breach. The Florida Incident involved a former FDIC employee who copied a large quantity of sensitive FDIC information, including personally identifiable information, to removable media and took this information when the employee departed the FDIC's employment in October 2015. The FDIC detected the incident through its DLP tool.

Audit Results

Although the FDIC had established various incident response policies, procedures, guidelines, and processes, these controls did not provide reasonable assurance that major incidents were identified and reported in a timely manner. Specifically, we found that:

- The FDIC's incident response policies, procedures, and guidelines did not address major incidents.
- The large volume of potential security violations identified by the DLP tool, together with limited resources devoted to reviewing these potential violations, hindered meaningful analysis of the information and the FDIC's ability to identify all security incidents, including major incidents.

Further, based on our analysis of the Florida Incident, we concluded that the FDIC had not properly applied the criteria in OMB Memorandum M-16-03 when it determined that the incident was not major. Specifically, the FDIC based its determination on various mitigation factors related to the "risk of harm" posed by the incident. Although such factors have relevance in determining the mitigation actions to be taken in addressing incidents, the factors are not among those listed in OMB Memorandum M-16-03 for agencies to consider when determining whether incidents are major and, therefore, are not relevant. We notified the CIO on February 19, 2016 that our analysis of the Florida Incident found that reasonable grounds existed to designate the incident as major as of December 2, 2015, and, as such, the incident warranted immediate reporting to the Congress. The FDIC subsequently reported the Florida Incident to the Congress as major on February 26, 2016.

When the FDIC did notify the Congress of the incident, certain risk mitigation factors in the notifications were either unsupported by adequate evidence and/or inconsistent with information available at the time. As a result, in our view, the notifications did not accurately portray the extent of risk associated with the incident. Our analysis of the Florida Incident also found that:

- More than 4 weeks had elapsed between the initial discovery of the incident and a determination that the incident was a breach.
- The decision about whether individuals and organizations potentially affected by the incident would be notified was untimely, and a required notification to another federal agency was not made.
- Records documenting investigative activities were not centrally managed and sometimes contained unreliable information, and the underlying rationale and discussions pertaining to certain decisions were not always documented.

The results of our analysis of the Florida Incident prompted the CIO to initiate a review of similarly-situated information security incidents that occurred after the OMB issued Memorandum M-16-03 to determine whether additional incidents warranted designation as major. The CIO's review resulted in six additional incidents being reported to the Congress as major between March and May 2016.

On May 5, 2016, the CIO provided our office with an outline of a plan describing a number of initiatives aimed at addressing policy and program shortcomings in the FDIC's incident response processes. Such initiatives include, but are not limited to, developing an overarching incident response program guide, hiring an incident response coordinator, implementing a new incident tracking system, updating incident response policies and procedures, and performing a comprehensive assessment of the FDIC's information security and privacy programs.

Recommendations and Corporation Comments

The report contains five recommendations addressed to the CIO that are intended to provide the FDIC with greater assurance that major incidents will be identified and reported consistent with FISMA and OMB Memorandum M-16-03. Addressing these recommendations will facilitate the Congress' ability to provide the oversight intended by FISMA and contribute to the OMB's goal of having effective inter-agency communication so that incidents are mitigated appropriately and as quickly as possible. FDIC management concurred with all five recommendations and described planned actions that were responsive.

Contents

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, Virginia 22226

Office of Audits and Evaluations
Office of Inspector General

DATE: July 7, 2016

MEMORANDUM TO: Lawrence Gross, Jr.
Chief Information Officer

/Signed/
FROM: Mark F. Mulholland
Assistant Inspector General for Audits

SUBJECT: *The FDIC's Process for Identifying and Reporting Major Information Security Incidents* (Report No. AUD-16-004)

This report presents the results of our audit of the FDIC's process for identifying and reporting major information security incidents (referred to herein as major incidents).[1] The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the FDIC, to develop procedures for notifying and consulting with, as appropriate, various Congressional Committees for major incidents. According to the statute, agencies are to notify the committees not later than 7 days after the date on which there is a reasonable basis to conclude that a major incident has occurred. The Office of Management and Budget's (OMB) Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements,* dated October 30, 2015, provides agencies with a definition of the term "major incident" and a framework for assessing whether an incident is major.

The objective of the audit was to determine whether the FDIC had established key controls that provide reasonable assurance that major incidents are identified and reported in a timely manner. The audit included an assessment of relevant FDIC incident response policies, procedures, and guidance; a review of the FDIC's implementation of its Data Loss Prevention (DLP) tool; and an analysis of investigation-related activities, records, decisions, and reports for one specific incident—FDIC Security Incident Number CINC-221387 (referred to herein as the Florida Incident).[2]

We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 of this report includes additional details about our objective, scope, and methodology; Appendix 2 contains a glossary of terms; Appendix 3 contains a list of abbreviations and acronyms; Appendix 4 contains the Corporation's comments; and Appendix 5 contains a summary of the Corporation's corrective actions.

---

[1] Certain terms that are underlined when first used in this report are defined in Appendix 2, *Glossary of Terms*.
[2] See Appendix 1, *Objective, Scope, and Methodology*, for a description of how we selected this incident for review.

Background

The federal government has experienced a marked increase in the number of information security incidents affecting the confidentiality, availability, and integrity of data, systems, and services. Such incidents can come from internal or external sources. Internal sources include employees or contractor personnel working within an organization who commit errors and fraudulent or malevolent acts. External sources include hackers, criminals, foreign states, terrorists, and other groups who execute cyber-based attacks. These threats underscore the criticality of establishing an effective, enterprise-wide information security program.

As the federal deposit insurer and regulator of state-chartered, nonmember financial institutions, the FDIC collects and manages a significant quantity of highly sensitive and business proprietary information on insured institutions and their customers. As an employer, an acquirer of services, and a receiver for failed financial institutions, the FDIC also obtains considerable amounts of sensitive information from its employees, its contractors, and the customers of failed institutions. Key to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system is safeguarding this information from unauthorized access or disclosure that could lead to financial harm to a financial institution, identity theft, consumer fraud, and potential legal liability or public embarrassment for the Corporation.

Agency Requirements for Reporting Major Incidents

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that includes (among other things) procedures for detecting, reporting, and responding to security incidents. Such procedures are to include notifying and consulting with, as appropriate, the Congressional Committees referenced in the statute for major incidents. According to FISMA, Congressional notification and consulting is to occur not later than 7 days after the date on which there is a reasonable basis to conclude that a major incident has occurred. In addition, agencies must, within a reasonable period of time after additional information about a major incident is discovered, provide further information to the Congressional Committees. FISMA also requires that the agency's annual report required under the statute include a description of each major incident or related sets of incidents.[3]

To promote consistency in agency reporting, FISMA requires OMB to develop guidance on what constitutes a major incident. Accordingly, OMB issued Memorandum M-16-03 on October 30, 2015 that provides agencies with a definition of the term "major incident" and a framework of factors, the combination of which agencies must consider

[3] The description is to include summaries of the threats and threat actors, vulnerabilities, and impacts relating to the incident; the risk assessments conducted of the affected systems before the date on which the incident occurred; the status of compliance of the affected systems with applicable security requirements at the time of the incident; and the detection, response, and remediation actions taken. For major incidents involving a breach of personally identifiable information (PII), agencies must also describe the number of individuals whose information was affected and the information that was breached or exposed.

when characterizing an incident as major.[4] The memorandum states that agencies should notify affected individuals, in accordance with FISMA, as "expeditiously as practical, without unreasonable delay." The memorandum adds that although agencies may consult with the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) when determining whether an incident is considered a "major incident," it is ultimately the responsibility of the victim agency to make the determination. The FDIC Legal Division has opined that OMB Memorandum M-16-03 is generally applicable to the Corporation.

The FDIC's Processes for Addressing Information Security Incidents

FDIC Circular 1360.12, *Reporting Computer Security Incidents*, dated June 26, 2003, defines a computer security incident as an event that threatens the security of an automated information system, including computers, the mainframe, networks, software, and associated equipment, and the data stored or transmitted using that equipment. Incidents can be identified through a variety of sources. For example, employees and contractors must contact the FDIC's Help Desk/Computer Security Incident Response Team (collectively referred to herein as CSIRT) to report a suspected security incident; technologies used by the FDIC to monitor network activity, such as the DLP tool, may identify apparent security policy violations; and outside organizations may notify the FDIC of illegal or suspicious activity involving the FDIC's information technology (IT) resources.

> Computer security incidents (which, for purposes of this report, have the same meaning as information security incidents) include such things as *denial of service* attacks that cause a system or service to become unavailable to authorized users; *malicious code*, such as a virus or worm, that infects an operating system or application; and *data breaches* that involve the unauthorized exfiltration of sensitive information. Any of these incidents have the potential to be major.

The Information Security and Privacy Staff (ISPS) within the Chief Information Officer (CIO) Organization has overall responsibility for analyzing, reporting, and remediating information security incidents. ISPS reports to the Acting Chief Information Security Officer (CISO), who reports to the CIO. The CIO reports to the FDIC Chairman. Other organizational components also play a role in addressing information security incidents. Most notably, CSIRT provides technical assistance and investigates, reports, resolves, and closes incidents by working with division and office Information Security Managers (ISM), Privacy Program Office staff, the Data Breach Management Team (DBMT) for data breaches, and others.

Our audit focused on the FDIC's processes for addressing one particular type of information security incident—a breach of sensitive information—because the incident we selected for detailed review (i.e., the Florida Incident) was a breach. The FDIC's *Data Breach Handling Guide,* Version 1.4, dated April 2015, defines a breach as an

[4] According to the OMB memorandum, the definition of the term major incident is subject to change by OMB based upon incidents, risks, recovery activities, or other relevant factors.

incident in which sensitive FDIC information, including business sensitive information and/or PII, has been lost, compromised, acquired, disclosed, or accessed without authorization, or any similar incident where persons other than authorized users and for other than authorized purposes, have access or potential access to sensitive information. The Guide contains detailed procedures for addressing data breaches and identifies eight separate stages of the incident handling lifecycle, consisting of preparation/prevention; discovery/detection; reporting; data collection, investigation, and escalation; analysis and mitigation; external breach notification; closure; and after action review/lessons learned. Table 1 describes three of these stages, which are pertinent to a proper understanding of our audit approach, findings, and conclusions. As described later, the FDIC had not updated the *Data Breach Handling Guide* to address the reporting of major incidents until June 2016.

Table 1: Selected Stages of the Incident Handling Lifecycle

Data Collection, Investigation, and Escalation*
During this stage, CSIRT gathers and documents pertinent information about the suspected or confirmed breach and notifies the affected division(s) and/or office(s). The ISM of the affected division(s) or office(s) and the Incident Response Point of Contact (or Incident Lead), which may also be the ISM, coordinate with ISPS to investigate, assess, and ensure compliance with regulatory directives and policies. An Incident Risk Analysis (IRA) (described more fully below) is also prepared. At this stage of the incident life cycle, the IRA records information about the incident and the FDIC's investigative activities and corrective actions.
Analysis and Mitigation
During this stage, the ISM and the Incident Lead work in coordination with ISPS to document a risk analysis for the incident in the IRA. The risk analysis considers such things as the nature of the data, the probability of its misuse, the likelihood that the incident may lead to harm, and the ability of the FDIC to mitigate harm. Based on the results of the risk analysis, a risk determination (i.e., an overall potential impact/risk level of low, moderate, or high) is documented in the IRA. Mitigation measures, including whether external notification is recommended to mitigate the harm posed by the incident, are recorded in the IRA. A decision is also made about whether to convene the DBMT. The DBMT is a cross divisional group of FDIC stakeholders that is responsible for (among other things) reviewing and verifying the IRA in terms of the level of harm posed to affected individuals/entities; determining and managing an appropriate course of action to respond to the breach and mitigate any harm; and recommending appropriate external breach communications and notifications. The DBMT is convened, facilitated, and managed by the ISPS employee designated to manage the incident on behalf of ISPS. The DBMT is usually convened if an incident is deemed significant based on the number of individuals impacted or the loss or compromise of critical sensitive information that may significantly affect the FDIC's mission or operations.
External Breach Notification
During this stage, notifications and credit monitoring services (if warranted) are provided to affected individuals and entities. The *Data Breach Handling Guide* states that, in general, the FDIC provides external notification and credit monitoring for incidents having an impact/risk level of moderate or high where Social Security Numbers (SSNs) or other sensitive information that could lead to identity theft has been compromised. The guide provides information about the content, timing, method, and recipients of notifications. The goal is to provide notifications to affected individuals and entities without unreasonable delay so they can take proactive steps quickly.

Source: OIG analysis of the *Data Breach Handling Guide*.

* In September 2015, the FDIC published the *FDIC Cyber Threat and Incident Escalation Guide* to provide a framework and standard operating procedures for escalating cyber threat or incident information from a division or office to FDIC executive management. The guide contains an FDIC *Incident Severity Schema* to help determine how quickly and to what levels threat or incident information should be escalated.

Timeline for the Florida Incident

A timeline of key activities associated with the Florida Incident follows.

October 23, 2015	The member of ISPS supporting the DLP tool notifies CSIRT of a suspected security incident. The activity description states that a former Bank Secrecy Act (BSA) specialist within the Division of Risk Management Supervision's (RMS) Gainesville, Florida, field office appeared to have copied a large quantity of sensitive information (i.e., more than 1,200 documents), including SSNs from customer bank data and other sensitive FDIC information, onto a single Universal Serial Bus (USB) storage device—a type of removable media. CSIRT, in turn, reports the incident to US-CERT. According to the Computer Security Incident Report prepared by CSIRT, the sensitive information appeared to include Suspicious Activity Reports (SARs), Bank Currency Transaction Reports, BSA Customer Data Reports, and a small subset of personal work and tax files. The report indicated that the BSA specialist had downloaded the information on September 16 and 17, 2015, and on October 15, 2015, prior to the employee's departure from FDIC employment on October 15, 2015. The member of ISPS supporting the DLP tool reports the incident to the FDIC Privacy Program Office. In addition, ISPS notifies RMS staff of the incident. RMS staff note that the former employee had turned in an encrypted USB device upon departure.
October 26, 2015	The former employee's supervisor contacts the employee to obtain the password for the USB device that was turned in at the time of departure, but the former employee cannot remember the password.
October 30, 2015	OMB issues Memorandum M-16-03.
November 2, 2015	The current CIO arrives at the FDIC.
November 3, 2015	After decrypting the USB device that the former employee turned in at departure, ISPS determines that the device is not the same device involved in the incident.
November 6, 2015	The FDIC requests assistance from the Office of Inspector General's (OIG) Office of Investigations (OI) to resolve the incident. On the same day, OI responds to FDIC staff by asking for additional information regarding the FDIC's investigative activities and whether the FDIC had asked the former employee to return the USB device in question.
November 9, 2015	ISPS determines that the USB device involved in the incident was personally-owned. FDIC Circular 1360.9, *Protecting Sensitive Information*, dated April 30, 2007, requires that sensitive electronic information be stored only on FDIC IT equipment.

November 10-17, 2015	RMS and ISPS provide the OIG with additional information on the FDIC's investigation of the incident and continue to request the OIG's assistance in handling the incident.
November 18, 2015	The DBMT holds the first of two meetings to discuss the facts of the incident and recommend actions.
November 19, 2015	Three separate discussions are held with the former employee on the same day wherein the employee repeatedly denies copying the information or owning a removable drive. Based on the former employee's response, an additional inquiry is made to OI regarding the potential for their involvement.
November 2015-December 2015	On or about November 20, 2015, and continuing into early December 2015, the OIG had a number of conversations with FDIC Legal Division staff and OIG staff communicated that they did not believe, at that time, that probable cause existed to secure a warrant to search the former employee's residence.[5] Therefore, the OIG informed FDIC staff that it was not prepared to send an agent to attempt to retrieve the USB device.
November 25, 2015	The DBMT holds a second meeting on the incident. The DBMT recommends in an incident summary report that the CIO classify the incident as a breach. In making the recommendation, the DBMT considered information contained in a detailed IRA that included, among other things, a description of the same type and volume of sensitive information as referenced in the Computer Security Incident Report, dated October 23, 2015. (The CIO informed us on June 27, 2016, that he had concurred with the DBMT's recommendation, as evidenced by the incident summary report.) The incident summary report indicates that additional work is needed to assess the impact level of the breach, and whether or not notification and credit monitoring to potentially affected parties would be required or recommended. The DBMT also recommends that (a) a face-to-face meeting be arranged with the former employee as an additional attempt to recover the USB device; (b) a legal demand letter be sent to the former employee if the face-to-face meeting is unsuccessful; and (c) RMS conduct further research to determine the count of PII records and obtain more specificity regarding the business sensitive information involved in the incident. The member of the ISPS supporting the DLP tool advises the Acting Privacy Program Manager and the ISPS Incident Lead that the DLP tool had identified over 90,000 potential SSNs in the downloads to the USB

[5] As a general matter, before a judge may issue a search warrant, there must be a finding of probable cause. The level of evidence that is required to demonstrate probable cause must be greater than "mere suspicion." The facts must demonstrate that a reasonable person would believe that the location which is the subject of the warrant contains evidence of a crime, the instrumentalities of a crime, contraband, or the fruits of a crime (e.g., stolen property).

	device and that a detailed analysis was needed to determine the number of individuals impacted.
December 2, 2015	RMS staff attempt a face-to-face meeting with the former employee, but the employee refuses to meet and refers the RMS staff to an attorney who represents the employee. The FDIC Legal Division then sends the former employee a letter demanding that the USB device be returned to the FDIC by December 8, 2015. On the same day, RMS staff determine that at least 10,000 unique SSNs were involved in the breach.
December 7, 2015	The CIO determines on behalf of the FDIC that the incident is not major.[6] The CIO's determination is noted in a DBMT Summary Report as of this date.
	The former employee's attorney informs FDIC Legal Division staff that the employee did, in fact, own the USB device referred to in the legal demand letter and that the device was in the attorney's possession.
December 8, 2015	The FDIC recovers the USB device used to download the sensitive information.
December 2015-April 2016	RMS and ISPS work to identify and document the total number of individuals and entities impacted by the breach. In addition, the Legal Division worked with the former employee's attorney to negotiate language that would be acceptable to the employee for inclusion in a written declaration from employee. On March 25, 2016, the former employee signed a declaration indicating that the employee had not disseminated or copied any confidential FDIC information from the USB device and that the employee no longer had possession, custody, or control of any confidential FDIC information in any format.
February 26, 2016	The FDIC notifies the Congress that a review of the incident by our office had identified reasonable grounds to designate the incident as major.

On April 7, 2016, ISPS provided us with an updated IRA for the Florida Incident. The IRA indicated that a total of 71,069 individuals and entities (consisting of 40,354 individuals and 30,715 banks and other entities) were potentially involved in the breach. In addition, a forensic analysis of the USB device completed in June 2016 by ISPS at our request found that 100,966 files were stored on the device. The forensic analysis also found indications that the USB device had been accessed after the employee's employment ended, but before the USB device had been returned to the FDIC.

[6] The FDIC had not updated its policies and procedures to address major incidents at the time of the CIO's determination. However, the CIO informed us that only the FDIC Chairman could designate an incident as major (based on a recommendation from the CIO, and in consultation with the Legal Division). The CIO advised us that since he determined on December 7, 2015 that grounds did not exist to designate the incident as major, the determination was not forwarded to the FDIC Chairman for review or approval.

Overall Results

Although the FDIC had established various incident response policies, procedures, guidelines, and processes, these controls did not provide reasonable assurance that major incidents were identified and reported in a timely manner. Specifically, we found that:

- The FDIC's incident response policies, procedures, and guidelines did not address major incidents.

- The large volume of potential security violations identified by the DLP tool, together with limited resources devoted to reviewing these potential violations, hindered meaningful analysis of the information and the FDIC's ability to identify all information security incidents, including major incidents.

Further, based on our analysis of the Florida Incident, we concluded that the FDIC had not properly applied the criteria in OMB Memorandum M-16-03 when it determined that the incident was not major. Specifically, the FDIC based its determination on various mitigation factors related to the "risk of harm" posed by the incident. Although such factors have relevance in determining the mitigation actions to be taken in addressing incidents, the factors are not among those listed in OMB Memorandum M-16-03 for agencies to consider when determining whether incidents are major and, therefore, are not relevant.

When the FDIC did notify the Congress of the incident, certain risk mitigation factors in the Congressional notifications were either unsupported by adequate evidence and/or inconsistent with information available at the time. As a result, in our view, the notifications did not accurately portray the extent of risk associated with the incident. Our analysis of the Florida Incident also found that:

- More than 4 weeks had elapsed between the initial discovery of the incident and a determination that the incident was a breach.

- The decision about whether individuals and organizations potentially affected by the incident would be notified was untimely, and a required notification to another federal agency was not made until after the OIG made FDIC aware of the requirement to notify the other agency.

- Records documenting investigative activities were not centrally managed and sometimes contained unreliable information, and the underlying rationale and discussions pertaining to certain decisions were not always documented.

The results of our analysis of the Florida Incident prompted the CIO to initiate a review of similarly-situated information security incidents that occurred after the OMB issued Memorandum M-16-03 to determine whether additional incidents warranted designation as major. The CIO's review resulted in six additional incidents being reported to the Congress as major between March and May 2016.

Our report contains five recommendations aimed at providing the FDIC with greater assurance that major incidents will be identified and reported consistent with FISMA and OMB Memorandum M-16-03. Addressing these recommendations will facilitate Congress' ability to provide the oversight intended by FISMA and contribute to the OMB's goal of having effective inter-agency communication so that incidents are mitigated appropriately and as quickly as possible.

On May 5, 2016, the CIO provided our office with an outline of a plan describing a number of initiatives aimed at addressing policy and program shortcomings in the FDIC's incident response processes. Such initiatives include, but are not limited to, developing an overarching incident response program guide, hiring an incident response coordinator, implementing a new incident tracking system, updating incident response policies and procedures, and performing a comprehensive assessment of the FDIC's information security and privacy programs.

Incident Response Policies, Procedures, and Guidelines Did Not Address Major Incidents

FISMA requires federal agencies to develop, document, and implement an information security program that includes, among other things, procedures for detecting, reporting, and responding to security incidents—including major incidents. Such procedures help to minimize loss and destruction to organizational resources when incidents occur. In addition, NIST Special Publication (SP) 800-61, Revision 2, *Computer Security Incident Handling Guide*, dated August 2012, states that written policies and procedures are an important component of any effective incident response capability. Further, up-to-date policies, procedures, and guidelines are an important internal control for ensuring that processes are repeatable, consistent, and effective, and for reducing operational risk associated with changes in staff.

Although the FDIC established various incident response policies, procedures, and guidelines,[7] they did not address major incidents, including:

- criteria, consistent with OMB Memorandum M-16-03, for determining whether an incident is major;
- roles and responsibilities for designating incidents as major;[8]

[7] Such policies, procedures, and guidelines included, for example, Circular 1360.12, *Reporting Computer Security Incidents*; the *Data Breach Handling Guide*; the *FDIC Cyber Threat and Incident Escalation Guide*; and procedures maintained by CSIRT for the prevention, detection, handling, analysis, response, recovery, and reporting of security incidents.

[8] Such roles and responsibilities extend beyond the CIO Organization. For example, the CIO informed us that only the FDIC Chairman could designate an incident as major (based on a recommendation from the CIO, and in consultation with the Legal Division).

- procedures for escalating incidents that have the potential for being major;
- guidelines for ensuring that key decisions on major incidents are made in a timely manner; or
- protocols for reporting major incidents internally and externally, including to appropriate Congressional Committees, and providing periodic updates, as warranted.

On December 23, 2015, ISPS updated the *Data Breach Handling Guide* to include information about major incidents as defined in OMB Memorandum M-16-03. The updated guide was posted to the FDIC's internal network on December 23, 2015. However, the CIO informed the OIG that he rescinded this version of the *Data Breach Handling Guide* in February 2016 because the update was made without his review or approval, or adequate input from other corporate stakeholders, such as the Legal Division and the Division of Administration's Human Resources Branch. At the close of our audit, the CIO was working with corporate stakeholders to conduct a comprehensive review of the *Data Breach Handling Guide* and update the roles, responsibilities, and procedures contained therein.[9]

The lack of written policies, procedures, and guidelines addressing major incidents as described in OMB Memorandum M-16-03 reduced the FDIC's assurance that major incidents would be identified and reported in a timely manner. It also contributed to confusion among FDIC staff—including the CIO, Acting CISO, Division of Information Technology (DIT) Director, and ISPS Incident Lead—regarding the procedures and protocols to be followed in resolving and reporting the Florida Incident.

Recommendation

We recommend that the CIO:

(1) Revise the FDIC's incident response policies, procedures, and guidelines to address major incidents.

The Data Loss Prevention Tool Can Be Better Leveraged to Identify Major Incidents

A number of organizations in both the public and private sectors have adopted data loss prevention technologies to help stem the loss of sensitive information from their organizations. The use of these technologies is a recognized best practice. The FDIC has implemented a commercially available data loss prevention solution, referred to herein as

[9] On June 13, 2016, the Acting CISO released Version 1.5 of the guide, dated June 6, 2016, that contained minor changes to reflect new requirements in FISMA and OMB Memorandum M-16-03. The Acting CISO indicated that additional substantive changes are being made to the guide to incorporate comments and edits submitted earlier in the year from key stakeholders.

the DLP tool, to help ensure that sensitive FDIC data are secured consistent with policy. The DLP tool monitors and inspects FDIC data in three primary states: (1) data at rest (i.e., network file shares), (2) data in motion (i.e., e-mails and Web uploads), and (3) data at endpoints (i.e., files copied to removable media). Potential security policy violations flagged by the DLP tool include the unauthorized exfiltration of sensitive data via removable media, the transmission of sensitive e-mails in an unencrypted format, and the failure to properly restrict access to internal network file shares.

As reflected in Table 2, the DLP tool identified 604,178 potential security policy violations (referred to herein as events) during the 6-month period ended February 29, 2016. The majority of these events were generated by employees or contractor personnel who copied sensitive information from the internal network to removable media (as was the case for the Florida Incident). Each event flagged by the DLP tool requires a manual review by ISPS to determine whether the event is a "false positive" (e.g., the use of removable media for a legitimate business practice) or warrants escalation to CSIRT for further investigation.

Table 2: Events Flagged by the DLP Tool and Referred to CSIRT from September 2015 through February 2016

Nature of Event	Number of Events
Removable Media (e.g., USB device/DVD/CD)	389,338
Network Events (E-mail/Web Uploads)	105,678
Open File Shares on the Internal Network	109,162
Total	**604,178**
Events Escalated to CSIRT	**Number of Events**
Endpoint DLP (including removable media)	29
Network DLP	59
File Shares DLP	3
Total	**91**

Source: OIG analysis of data provided by ISPS.

The significant volume of removable media events flagged by the DLP tool, together with limited resources devoted to reviewing these events (i.e., one individual), prevented ISPS from analyzing the vast majority of removable media events. In response to this situation, ISPS personnel informed us that they limited manual reviews of USB-related events to those involving recently departed employees and contractor personnel because there is inherently higher risk of data exfiltration associated with departing personnel. The individual in ISPS responsible for managing the DLP tool identified several factors that contributed to the high volume of events identified by the DLP tool. A summary of these factors follows.

Expanded Use of the DLP Tool. Beginning in September 2015, the FDIC configured the DLP tool to begin monitoring sensitive data copied from the internal network to removable media. This resulted in a significant increase in the number of events flagged by the tool. The CIO informed us that, in his view, the expanded use of the DLP tool was implemented without adequate planning or consideration of the impact on existing resources. The CIO also indicated that the use of removable media was known to be a common practice at the FDIC and, as a result, it could have been anticipated that a

significant increase in removable media events would occur when the DLP tool was configured to begin reviewing the copying of data to removable media.

Prevalent Use of Removable Media. Prior to March 18, 2016, few restrictions were placed on employees and contractor personnel from copying information from the corporate network to corporate-owned removable media.[10] The FDIC Chairman notified all employees and contractor personnel that, effective March 18, 2016, they were no longer permitted to copy data to any removable media, except in cases approved by an FDIC division or office director. In addition, the FDIC Chairman's communication indicated that work had begun to change underlying business processes to eliminate the need for removable media (to the extent practical) for those processes that require the use of removable media. As of June 28, 2016, DIT officials reported that 1,089 of 16,922 (or 6 percent) network accounts had permission to copy information to removable media. That number was expected to decrease as efforts to reduce the use of removable media continue.

Lack of Data Classification Standards. The DLP tool generates an event each time a user copies data from the internal network to removable media that includes pre-defined keywords or patterns of information. ISPS coordinates with the FDIC's business units on a periodic basis to establish these keywords and pattern filters. However, the individual in ISPS responsible for managing the DLP tool indicated that the effectiveness of this effort has been limited because the FDIC has not yet established corporate-wide data classification standards that define how data should be safeguarded.[11] In addition, the FDIC had not yet completed ongoing efforts to identify its high value assets as prescribed in OMB's Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, dated October 30, 2015.

A review of data classification standards and the FDIC's efforts to identify high value assets was not within the scope of this audit. However, the establishment of such standards and the identification of high value assets should better enable the FDIC to focus its data loss prevention efforts, including the DLP tool, on the Corporation's most sensitive information.

---

[10] A notable exception was FDIC employees with access to resolution plans submitted to the FDIC pursuant to section 165(d) of the Dodd-Frank Wall Street Reform and Consumer Protection Act. In 2013, the FDIC implemented a technical security control to prohibit these employees from copying information to removable media. However, as discussed in our report, entitled *The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans* (Report No. AUD-16-003, dated July 6, 2016), this control was not always effective in prohibiting employees form copying resolution plans to USB devices.

[11] An ongoing government-wide initiative called the Controlled Unclassified Information (CUI) Program is being led by the National Archives and Records Administration (NARA) pursuant to Executive Order 13556, *Controlled Unclassified Information*, to standardize and simplify the manner in which the Executive branch handles unclassified information that requires safeguarding or dissemination controls. The CUI Program is intended to address the current inefficient and confusing patchwork that leads to inconsistent marking and safeguarding as well as restrictive dissemination policies. In May 2015, NARA's Information Security Oversight Office issued a proposed rule to establish policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the CUI Program. As of June 2016, a final rule had not been published.

Recommendation

We recommend that the CIO:

(2) Review the current implementation of the DLP tool, including the keywords and filters used to monitor data, procedures for assessing output, and resource commitments, to determine how the tool can be better leveraged to safeguard sensitive FDIC information. As part of this effort, consider planned and ongoing efforts related to data classification standards and the identification and protection of high value assets.

The FDIC Did Not Properly Apply OMB Guidance in Its Evaluation and Reporting of the Florida Incident

FISMA states that agencies must notify and consult with, as appropriate, the Congressional Committees referenced in the statute for major incidents. In addition, OMB Memorandum M-16-03 provides agencies with a definition of the term major incident and a framework of factors, the combination of which agencies must consider when assessing whether an incident is major.

We concluded that the CIO did not properly apply the criteria in OMB Memorandum M-16-03 in determining that the Florida Incident was not major in December 2015. Specifically, the CIO's determination was based on risk mitigation factors that are not addressed in OMB Memorandum M-16-03 and, therefore, are not relevant to the determination. Once the FDIC did notify Congressional Committees of the incident, certain risk mitigation factors in the notifications were either unsupported by adequate evidence and/or inconsistent with information available at the time. As a result, in our view, the notifications did not accurately portray the extent of risk associated with the incident.

We also found that substantial time had elapsed between the initial discovery of the Florida Incident and a determination that the incident was a breach. In addition, a decision about whether individuals and organizations potentially affected by the breach should be notified was untimely, and a required notification to another federal agency was not made. A detailed discussion of these matters follows.

OIG Analysis of the Florida Incident

According to OMB Memorandum M-16-03, a major incident will be characterized by a combination of the following factors:

(1) involves information that is Classified, CUI proprietary, CUI Privacy, or CUI Other; *and*

(2) is not recoverable, not recoverable within a specified amount of time, or is recoverable only with supplemental resources; *and*

(3) has a high or medium functional impact to the mission of an agency; *or*

(4) involves the exfiltration, modification, deletion or unauthorized access or lack of availability to information or systems within certain parameters to include either:

a) a specific threshold of number of records or users affected;[12] or

b) any record of special importance.[13]

We reviewed the facts and circumstances pertaining to the Florida Incident and determined that it satisfied three of the above referenced factors and, therefore, was major. Table 3 provides the details of our analysis.

Table 3: OIG Analysis of the Florida Incident Relative to OMB Memorandum M-16-03

Factor	OMB Definition	Characteristics of the Incident That Satisfy the Factor	Factor Met?
CUI Privacy	The confidentiality of personal information, or in some cases, PII, as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007, or "means of identification" as defined in 18 USC 1028 (d)(7).	On October 23, 2015, the DLP tool identified that potentially 1,200 documents including SSNs and bank data were copied to a USB device by a then-departed employee. An IRA completed on or about November 25, 2015 stated that the incident included more than 1,200 documents and zip files including SSNs. In addition, the IRA noted that the files contained customer bank data with SSNs, SARs, Bank Currency Transaction Reports, and a small subset of data containing personal work and tax files of the former employee. Further, on December 2, 2015, the FDIC confirmed that at least 10,000 unique SSNs were included in the former employee's data download(s).	✓

[12] OMB Memorandum M-16-03 defines these thresholds as 10,000 or more records or 10,000 or more users affected.

[13] OMB Memorandum M-16-03 defines a record of special importance as any record that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in a significant or demonstrable impact onto agency mission, public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. OMB Memorandum M-16-03 further states that a collection of records of special importance in the aggregate could be considered an agency high value asset.

Factor	OMB Definition	Characteristics of the Incident That Satisfy the Factor	Factor Met?
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly). (If this information was exfiltrated, changed, deleted, or otherwise compromised, then the incident is considered major if either 10,000 or more records or records of special importance were affected.)	The information included records of special importance (e.g., SARs) likely to result in a significant and demonstrable impact to public confidence if disclosed. It also included more than 10,000 SSNs downloaded to a personal, unencrypted and non-password protected USB device that was removed from the FDIC's premises without authorization for a period of almost 2 months. It is not possible for the FDIC to determine whether the information was compromised prior to return of the USB device to the FDIC on December 8, 2015.	✓
Exfiltration	To obtain, without authorization or in excess of authorized access, information from a system without modifying or deleting it.	The access became unauthorized when the employee departed from the FDIC. The information was taken, unencrypted and via an unauthorized device, off of the FDIC's premises.	✓

Source : OIG analysis of the application of factors in OMB Memorandum M-16-03 to the Florida Incident.

Our analysis also found that reasonable grounds existed to designate the incident as major as of December 2, 2015, and, as such, the incident should have been reported to the Congress not later than December 9, 2015.[14] Moreover, it is possible that the incident could have been designated as major as early as November 6, 2015 (7 days after OMB issued its Memorandum M-16-03) as the exfiltration involved records that had special importance.[15] We notified the CIO of the results of our analysis in a memorandum dated February 19, 2016. The FDIC Chairman subsequently reported the Florida Incident to the Congress as major on February 26, 2016.

[14] We independently verified that at least 10,000 unique SSNs were involved in the breach. We also noted that the SSNs were often associated with other PII, such as bank account numbers, names, and addresses. In addition, the information we reviewed included Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) suspect lists, copies of drivers' licenses, passports, tax returns, State of Florida reports of examination, FDIC enforcement actions, bank wire logs, and green cards.

[15] The information downloaded by the employee included SARs. Inappropriate disclosure of a SAR to an unauthorized person is a violation of federal law. Such disclosure could result in significant or demonstrable impact to public confidence in the FDIC's ability to protect personal information since SARs often contain PII. The FDIC's IRA prepared on or about November 25, 2015 noted that the downloaded information could be used to open new accounts or commit identity theft, and could be used to cause public/reputational embarrassment, jeopardize the mission of FDIC, or cause other harm.

The FDIC's Evaluation of the Florida Incident

The CIO made a determination in December 2015 that the Florida Incident was not major.[16] The determination was recorded in a December 7, 2015 DBMT Summary Report, which stated, in part "Based on the recommendation of the DBMT [that the incident be declared a breach] and the supporting chronology, the Chief Information Officer concurs with the recommendation of the DBMT. However, after careful review of the Office of Management and Budget, Memorandum 16-03, dated October 30, 2015, [the CIO] does not recommend classification of the incident as a major incident."

The CIO informed us that he considered a number of factors in determining whether the Florida Incident was major. Such factors included the criteria contained in OMB Memorandum M-16-03; information that was available at that time about the incident; the DBMT's November 25, 2015 recommendation; information security guidance; and the following risk mitigation factors:

- the employee had legitimate access to the data while employed at the FDIC;
- a view that the employee had inadvertently downloaded the information when attempting to download personal information in preparation for departure because the employee was not computer proficient;
- there was no evidence that the employee had disseminated the data;
- the relationship with the employee had not been adversarial;
- the FDIC recovered the information from the employee; and
- the employee was working through significant personal issues, presenting a distraction for the employee.

The CIO and other senior FDIC executives informed us that, in their view, it was reasonable to consider the "risk of harm" to individuals and entities when determining whether the Florida Incident was major. These officials noted that FISMA broadly discusses agency responsibilities for assessing the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems. In addition, NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*, references mitigating factors

[16] The CIO informed us that his determination not to classify the Florida Incident as major as of December 7, 2015 was based on information that was available at the time, and that his determination could have changed if information subsequently came to light warranting a recommendation that the incident be classified as major. As previously stated, the FDIC had not updated its policies and procedures to address major security incidents at the time the CIO's determination was made. However, the CIO informed us that only the FDIC Chairman could designate a security incident as major (based on a recommendation from the CIO, and in consultation with the Legal Division). The CIO also advised us that since he determined that the incident was not major as of December 7, 2015, his determination was not forwarded to the FDIC Chairman for review or approval.

and states that organizations can mitigate the impact of incidents by containing them and ultimately recovering from them.

The CIO informed us in February 2016 that absent the application of risk mitigation factors, such as those described earlier, the FDIC may be required to report too many incidents as major. The CIO referenced this point during a May 2016 Congressional hearing wherein he explained that not applying such risk mitigation factors could create an environment wherein everything is being reported as major, presenting a risk that significant events could be overlooked. The CIO referred to OMB Memorandum M-16-03, which states that it is the responsibility of the victim agency to make the determination as to whether an incident is major.

The CIO informed us that he discussed his recommendation that the Florida Incident was not major with the Deputy to the Chairman, Chief Operating Officer, and Chief of Staff; the Deputy General Counsel; and a representative of the Office of Legislative Affairs. The discussion was held on or about December 7, 2015. The CIO informed us that the factors in OMB Memorandum M-16-03 were considered and weighted against the risk mitigation factors described earlier. The CIO stated that the meeting participants expressed no concern with the proposed recommendation.[17] According to the CIO's written statement to the Congress in May 2016, the CIO judged the risk of harm for the Florida Incident to be very low based on the first five risk mitigation factors described earlier, meaning that reporting of the incident would fall under the FDIC's annual FISMA reporting requirement to the Congress.[18]

The Application of Risk Mitigation Factors Are Not Relevant to the Determination of Whether an Incident Is Major

The risk mitigation factors described above are not part of the classification criteria for a major incident as defined in OMB Memorandum M-16-03. Therefore, we determined that the factors were not relevant to a determination of whether the Florida Incident was major. Notably, the CIO's view that the risk of harm associated with the Florida Incident was very low at the time the incident was determined not to be major in December 2015 appears to have been premature. At that time, the FDIC was still working to assess the impact/risk level of the Florida Incident and the DBMT had not yet reached consensus on a final impact/risk level for the incident. The FDIC's records indicate that the DBMT met on April 4, 2016 and recommended at that time that the final impact/risk level be classified as low.[19]

---

[17] Although not required, we noted that a written legal analysis supporting the recommendation had not been prepared. In addition, the CIO informed us that the FDIC had not consulted with the OMB or US-CERT in making the determination that the incident was not major.

[18] The Florida Incident was not included in the FDIC's Fiscal Year 2015 FISMA submission because the information in the FISMA submission was as of September 30, 2015 and the Florida Incident was not detected until October 23, 2015.

[19] According to the IRA template, the risk of harm is low if the incident could result in limited or no harm, embarrassment, inconvenience, or unfairness to individuals or entities, or could have limited or no adverse effect on organizational operations, missions, or assets.

The concept of "risk of harm" is relevant to determining the appropriate course of action to mitigate risks associated with a breach, such as determining whether affected individuals or entities should be notified and/or offered credit monitoring services. Using the risk mitigation factors described earlier as criteria for determining whether an incident is major creates practical problems. For example, it is not practical to determine with a reasonable degree of certainty an individual's intent or motivation behind an exfiltration of sensitive information in light of the 7-day reporting requirement in FISMA. Attempts to do so run contrary to government-wide incident reporting requirements and guidelines that promote transparency and prompt notification. Both FISMA and US-CERT's *Federal Incident Notification Guidelines* indicate that agencies should not delay reporting in order to provide further details about incidents. Rather, agencies should provide follow-up reports that capture new information as investigative activities continue.

Congressional Notifications Referenced Certain Risk Mitigation Factors That Were Either Unsupported and/or Inconsistent with Available Information

Although FISMA and OMB Memorandum M-16-03 require agencies to notify the Congress of major incidents, the statute and guidance do not specify the exact type of information that should be included in the initial notifications. Accordingly, determining the content of the notifications is a matter of professional judgment. Nevertheless, information contained in notifications should be current, accurate, and complete. Further, any analysis or conclusions should be supported by sufficient, appropriate evidence, and any key assumptions or limitations should be properly disclosed. Such an approach helps to ensure that the recipients of the notifications have a proper understanding of the context, risk, and significance of the matters discussed.

In a letter dated February 26, 2016, the FDIC Chairman provided the Congressional Committees referenced in FISMA with a report from the Corporation's CIO indicating that the Florida Incident was major. The report described the facts and circumstances related to the Florida Incident as well as several risk mitigation factors. Although the facts of the Florida Incident were generally accurate, we determined that several of the risk mitigation factors cited in the report were either unsupported by adequate evidence and/or inconsistent with information available at the time. As a result, in our view, the notifications did not accurately portray the extent of risk associated with the incident. Our analysis of these risk mitigation factors is summarized in Table 4.

Table 4: OIG Analysis of Selected Risk Mitigation Factors Cited in Congressional Notification Letters

Risk Mitigation Factor and the CIO's Basis for Citing the Factor	OIG Analysis
The FDIC's investigation does not indicate that any sensitive information has been disseminated or compromised. The CIO informed us that the former employee's attorney	• The information involved in the breach was stored on a personally-owned USB device, in an unencrypted format, and without password protection. Consequently, the information was accessible to anyone who had access to the device. The device was recovered from the former employee's attorney. Therefore, it was accessible by at least one person other than the employee.

indicated that the employee would be willing to sign an affidavit* stating that the employee had not disseminated or copied any confidential FDIC information from the personal USB device and no longer had possession of confidential FDIC information.	• The information was outside of the FDIC's control for almost 2 months. No technical means exist to ensure that the information was not accessed by, or and disseminated to, others. • At the time of the congressional notification, the FDIC's forensic review of the USB device was limited to verifying that the serial number of the device and its contents matched the information collected by the DLP tool. The FDIC had not analyzed the USB device to determine whether there was evidence that the information had been accessed, copied, transmitted, or altered after the employee left the FDIC's employment. When appropriate, such an analysis can be a prudent investigative step to assess the risk of data dissemination or compromise. • A forensic review that was completed by ISPS, at our request, in June 2016 found that the USB device had been accessed subsequent to the employee's departure—which constituted unauthorized access.

Evidence suggests that the sensitive information was downloaded inadvertently and without malicious intent.
 	
The CIO informed us that the employee downloaded the information while attempting to download personal information in preparation for departure. The CIO stated it was his "inclination" that the employee was not computer literate and accidentally copied an entire library of files to the portable storage device.
	• The former employee submitted a resume when applying to the FDIC in August 2013 that identified classes taken towards a Master of Arts in IT management. The resume was contained in the employee's personnel file. We verified that the employee received the degree in March 2013. Further, on February 17, 2016 (prior to the Congressional notification), we informed the CIO that we had performed an Internet search of the former employee's name and identified a public Web page listing various IT courses that the employee had taken, suggesting that the employee was familiar with IT concepts and principles.
	
	• A forensic review of the USB device completed by ISPS, at our request, in June 2016 found that:
	
	  • The employee had set up two folders on the USB device—one for personal documents and another for FDIC documents. In addition, files were labeled with bank names or the types of bank data in the files. The limited amount of personal data that was downloaded was labeled with the former employee's first name and the type of data the file contained.
	
	  • The employee copied a significant quantity of information from an FDIC laptop on multiple occasions prior to the employee's last day of employment. In one instance, data was downloaded for approximately 14 consecutive hours.
	
	• In November 2015, the employee's former supervisor expressed concern to the FDIC team investigating the Florida Incident about the content of the files downloaded and the fact that many of the files were downloaded on the employee's last day of employment, which the supervisor believed may have indicated suspicious activity.

	• The IRA provided to us on April 7, 2016 states "The motivation for the downloading of the data is not known." • It is not possible to determine what the former employee's intent was at the time the information was downloaded onto the USB device. In our view, statements that an action was inadvertent or taken without malicious intent limit the FDIC's ability to successfully pursue civil or criminal remedies against the employee.
The FDIC's relationship with the employee has not been adversarial, and the individual has indicated that they would be willing to sign an affidavit attesting to the fact that the information has not been further disseminated or compromised. The CIO informed us that the former employee departed from the FDIC under amicable conditions. In addition, information obtained from the prior employee's supervisor and co-workers and the employee's signing of an affidavit demonstrate that the relationship with the employee was non-adversarial and remained so after her employment ended.	• The former employee was not forthright with the FDIC when attempts were made to recover the information. Specifically, the employee denied copying the information or owning a portable storage device during three separate discussions with the FDIC on November 19, 2015. The employee also refused to hold a face-to-face meeting with FDIC personnel to resolve the issue. When these efforts to recover the USB device were unsuccessful, the FDIC sent the former employee's attorney a letter demanding that the USB device be returned to the FDIC not later than December 8, 2015. • Following discussions with the former employee and the employee's attorney, the employee signed a declaration on March 25, 2016 representing that the employee had not disseminated or copied any confidential FDIC information from the USB device and that the employee no longer had possession, custody, or control of any confidential FDIC information in any format. Notably, the employee also signed FDIC Form 2150/01, *Pre-Exit Clearance Record for Employees*, on October 15, 2015, falsely certifying that the employee did not possess sensitive information and that no sensitive information would be taken from the FDIC upon the employee's departure.[20]

Source: OIG analysis of investigative records, correspondence, and testimony related to the Florida Incident.

* Subsequent to the Congressional notification, the employee voluntarily signed a written declaration. A declaration is not an affidavit (i.e., a sworn statement of fact under an oath or affirmation administered by a person authorized to do so by law).

Following our analysis of the Florida Incident, the FDIC conducted a review of prior incidents, six of which were subsequently reported as major to the Congress between March and May 2016. Although we did not conduct a detailed examination of the FDIC's reporting of these incidents, we noted that the associated notifications included risk mitigation factors that were similar to those included in the notification letters for the Florida Incident (e.g., the employees were not adversarial, evidence suggested that the sensitive information was downloaded inadvertently and without malicious intent, and

[20] FDIC Circular 2150.1, *Pre-Exit Clearance Procedures for FDIC Employees*, defines procedures for safeguarding FDIC-owned property and interests when employees leave the Corporation. A key component of these procedures is Form 2150/01, *Pre-Exit Clearance Record for Employees*.

the employees had signed an "affidavit" that the data had been in their sole possession and not disseminated in any way).

When mitigating factors are included in congressional notifications, it is prudent to ensure that appropriate aggravating factors are also included, both to promote transparency and to ensure that the incidents are portrayed in a proper context. Absent such information, an uninformed reader may misunderstand the nature and severity of the incident.

Timeliness of Incident Response Process

Our analysis of the Florida Incident found that key decisions were not made in a timely manner. Specifically, more than 4 weeks lapsed[21] between the initial discovery that the former employee had copied significant quantities of sensitive information onto a USB device and a determination by the CIO that the Florida Incident was a breach. In addition, the FDIC made a decision on April 4, 2016 not to notify individuals and entities that were potentially impacted by the breach—more than 5 months after the incident was initially discovered. At the close of our audit, FDIC management officials informed us that they had decided to reverse this decision and now plan to offer credit monitoring to those persons whose information was involved in the recently reported major incidents.

Adequacy of Notifying Potentially Affected Individuals and Entities

Although the scope of the audit did not include a review of the FDIC's processes for notifying individuals and organizations potentially affected by the Florida Incident, it came to our attention that the FDIC had not notified the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) that BSA information was involved in the breach. The FDIC has an interagency agreement with FinCEN that states, in part "the Agency [the FDIC] shall notify FinCEN immediately if the Agency...discovers any unauthorized use or access to BSA information, whether by Authorized Agency Personnel or otherwise." We notified members of the DBMT of this apparent noncompliance with the agreement on April 12, 2016. The FDIC notified FinCEN of the breach approximately 1 month later on May 18, 2016. We may review the FDIC's processes for notifying individuals and entities potentially affected by breaches as part of a separate assignment.

[21] Our review of FDIC documentation identified conflicting information regarding when the CIO determined that a breach had occurred in the Florida incident. While the CIO informed us that he declared the incident a breach on November 25, 2015, as evidenced by the November 25, 2015, DBMT incident summary report, other documentation obtained by the OIG indicates that there was confusion among staff regarding whether a breach had been formally declared by the CIO. For example, on November 30, 2015, the former CISO informed the CIO via email that the DBMT was waiting for the CIO to formally declare the Florida Incident a breach. Therefore, the OIG conservatively calculated the 4-week timeframe from the date that the FDIC discovered the incident (i.e., October 23, 2015) until the time that the CIO stated he concurred with the DBMT's recommendation on November 25, 2015.

Recommendations

We recommend that the CIO:

(3) Ensure that the revisions to the FDIC's incident response policies and procedures addressed in Recommendation 1 of this report include criteria for determining whether an incident is major consistent with FISMA and OMB Memorandum M-16-03.

(4) Establish controls to ensure that future Congressional notifications of major incidents include appropriate context regarding the risks associated with those incidents and that statements of risk are supported by sufficient, appropriate evidence.

Management of Investigative Records and Related Documentation Needed Improvement

FDIC Circular 4010.3, *FDIC Enterprise Risk Management Program*, states that internal controls, all transactions, and other significant events shall be clearly documented and that the documentation shall be readily available for examination. In addition, GAO's *Standards for Internal Control in the Federal Government* provide guidance on the appropriate documentation of transactions and internal control. The guidance notes that all transactions and other significant events need to be clearly documented and that documentation and records should be properly managed and maintained.

Our review of the FDIC's handling of the Florida Incident found that investigative records were not centrally managed and sometimes contained unreliable information. In addition, the rationale supporting certain decision-making pertaining to the Florida Incident and related discussions were not always recorded. In our view, a contributing cause for these issues was that the FDIC's incident response policies, procedures, and guidelines did not specifically address the management and storage of records. Several examples follow.

- **Records Not Centrally Managed.** Documents, analyses, and communications related to the Florida Incident were not maintained in a central, readily-accessible location. Instead, these records were maintained by various stakeholders involved in addressing the incident. For example, the Acting CISO, the Acting Privacy Program Manager, and the ISPS Incident Lead were not able to answer our questions about whether congressional notifications were made for the Florida Incident because these individuals did not receive copies of the letters. We provided the Acting CISO with copies of the FDIC's Congressional notification letters for two major incidents at the Acting CISO's request. In addition, the ISPS Incident Lead for the Florida Incident did not always have access to the most current IRA because the ISM investigating the incident maintained the working

copy of the document. As a result, the Incident Lead was not able to promptly respond to some of our questions.

- **IRA Contained Some Information That Was Unreliable.** An IRA provided to us on March 2, 2016, indicated that RMS and ISPS personnel were awaiting approval from the Chairman's Office to declare the Florida Incident a breach during the period December 14, 2015 through February 1, 2016. However, the CIO informed us that he had declared the Florida Incident a breach on November 25, 2015.

  In addition, the March 2, 2016 IRA stated that the FDIC had not discovered that the information on the former employee's USB device was accessed, viewed, disclosed, or distributed to unauthorized parties. However, a forensic analysis to support this statement had not been performed. The FDIC's December 2, 2015 legal demand letter to the former employee stated that once the USB device was returned to the FDIC, it would be analyzed as necessary to determine whether the data had been accessed, copied, transmitted, or altered in any way. A senior forensic specialist in ISPS informed us that during the FDIC's investigation of the Florida Incident, the analysis of the former employee's USB device was limited to verifying that it was the device in question and that the contents of the device were consistent with the information collected by the DLP tool. A forensic analysis completed by ISPS at our request in June 2016 found that FDIC files stored on the USB device had been accessed subsequent to the employee's departure—which constituted unauthorized access. In addition, the former employee had provided the unencrypted USB device to the employee's attorney—an individual who did not have authorization to access the device.

  The statement in the IRA that the FDIC had not discovered that the information on the USB device was accessed, viewed, disclosed, or distributed to unauthorized parties is relevant to the determination of the impact/risk level of the breach and whether external notification and/or credit monitoring to affected individuals and entities is warranted. As previously stated, the FDIC subsequently assigned an impact/risk level of "low" to the Florida Incident and initially decided not to notify affected individuals and entities or to provide credit monitoring. However, the FDIC now plans to offer credit monitoring to those persons whose information was involved in the recently reported major incidents.

- **Rationale Supporting Key Decision and Related Discussion Not Documented.** The CIO documented the recommendation that the Florida Incident not be designated as major in a December 7, 2015 DBMT Summary Report. However, the DBMT Summary Report did not discuss the rationale supporting the recommendation or the factors that were used in determining that the Florida Incident was not major. Notably, the ISPS Incident Lead expressed concern to the Acting CISO in a January 26, 2016 email that the basis for the CIO's determination that (a) the risk associated with the incident was minor and (b) the

incident was not major had not been conveyed to him or the DBMT—50 days after those determinations had been made.

The CIO informed us that he discussed his recommendation that the Florida Incident not be designated as major on or about December 7, 2015 with the Deputy to the Chairman, Chief Operating Officer, and Chief of Staff; the Deputy General Counsel; and a representative of the Office of Legislative Affairs. The CIO informed us that the participants expressed no concern with the proposed recommendation and that a decision was made not to designate the Florida Incident as major. The CIO was unable to provide any documentation pertaining to this discussion.

The CIO acknowledged during our audit that investigative records needed to be centrally managed and that the content and reliability of records related to incidents needed improvement. Further, the CIO had expressed concern to CIO Organization and ISPS staff about inadequate documentation of the FDIC's investigative activities in several IRAs; the need to revise the IRA template to address Congressional notification based on new OMB guidance; the need to provide daily status updates on the Florida Incident to keep leadership apprised due to the seriousness of the incident; the lack of clear roles and responsibilities in handling certain aspects of the FDIC's investigation of the Florida Incident; and the need for clarification regarding the purpose and role of the DBMT. The CIO indicated that these weaknesses negatively affected the flow of information and communications among stakeholders and that making improvements in this area has been a priority for the CIO since his arrival at the FDIC in November 2015.

Improved record keeping will help ensure that information is readily available to those who need it; mitigate the risks associated with staff departures and changes; and better enable the FDIC to respond to inquiries. Further, investigative records, such as IRAs, can serve as evidence in criminal or civil proceedings. Accordingly, it is critical that they contain reliable information.

Recommendation

We recommend that the CIO:

(5) Review and update, as appropriate, incident response policies, procedures, and guidelines to require that (a) documentation related to investigation activities and decision-making is properly recorded and centrally maintained, (b) IRAs contain current, accurate, and complete information throughout the investigation supported by sufficient, appropriate evidence, and (c) the underlying analyses for key decisions and discussions are adequately documented.

The FDIC's Plans and Actions to Strengthen Controls Related to Major Incidents

As stated earlier, we conveyed the results of our analysis of the Florida Incident to the CIO in a memorandum, dated February 19, 2016. The memorandum stated that the FDIC was in apparent noncompliance with FISMA and related OMB guidance in connection with its initial determination that the Florida Incident was not major. Specifically, our analysis found that reasonable grounds existed to designate the Florida Incident as major as of December 2, 2015, and, as such, the incident needed to be immediately reported to the Congress. In addition, the memorandum stated that improvement was needed in the FDIC's process for identifying and reporting major incidents, including the elapsed time between the initial discovery of the Florida Incident and key decisions. The memorandum added that the FDIC should place priority attention on making a decision with respect to whether affected individuals and/or organizations would be notified, including whether such notification should be made incrementally as investigative activities continue.

In a memorandum dated February 24, 2016, the CIO informed our office that after reviewing our February 19, 2016 memorandum, carefully considering the analysis presented, and out of an abundance of caution, the FDIC would immediately notify the appropriate Congressional Committees about the Florida Incident. Those notifications were made on February 26, 2016. The CIO also committed to developing a plan within 60 business days to address the concerns raised in our February 19, 2016 memorandum (see below for more information on the plan). Further, the CIO indicated that a retroactive review of other incidents that had occurred after the issuance of OMB Memorandum M-16-03 would be conducted.[22] As reflected in Table 5, the CIO's review resulted in six additional major incidents being reported between March and May 2016.

Table 5: Major Incidents Reported by the FDIC to the Congress Between March and May 2016

	Date FDIC Became Aware of the Incident	Number of Records Involved (as of the date the incident was reported to the Congress)	Date Reported to the Congress
1	February 29, 2016	A former employee* copied sensitive information, including customer data for over 44,000 individuals.	March 18, 2016
2	January 8, 2016	A former employee copied 2,000 sensitive records, including customer data for over 15,000 individuals.	May 9, 2016**
3	November 10, 2015	A former employee copied approximately 1,200 sensitive records, including customer data for over 13,000 individuals.	May 9, 2016
4	December 10, 2015	A former employee copied sensitive information, including customer data for over 49,000 individuals.	May 9, 2016***
5	January 7, 2016	A former employee copied approximately 3,000 sensitive records, including bank customer data for over 18,000 individuals.	May 9, 2016

[22]The FDIC indicated that it used criteria established by the OIG in conducting its retroactive review of security incidents. The analysis and conclusions we reached in connection with our review of the Florida Incident were based on FISMA and OMB guidance, as well as the facts and circumstances of the incident. Our analysis and conclusions were not based on criteria that we independently established.

	Date FDIC Became Aware of the Incident	Number of Records Involved (as of the date the incident was reported to the Congress)	Date Reported to the Congress
6	November 10, 2015	A former employee copied approximately 500 sensitive records, including customer data for over 10,000 individuals.	May 9, 2016

Source: OIG review of the CIO's memoranda dated March 18, 2016 and May 9, 2016, to the FDIC Chairman summarizing the results of his retroactive review of FDIC security incidents.

* It should be noted that the major security incidents reported to Congress between March and May 2016 involved former employees that copied sensitive information prior to departing the FDIC.
** RMS notified the CIO and Acting CISO on April 27, 2016 that more than 10,000 individuals were potentially affected by the incident.
***According to the IRA, this incident was determined to be major as of March 28, 2016 but was not reported to the Congress until May 9, 2016 along with four other incidents.

In a memorandum dated May 5, 2016, the CIO provided our office with an outline of a plan to address shortcomings in the FDIC's information security program, including incident management response. The outline described the following corrective actions that were either initiated or planned to be initiated within the next 60-90 days:

- A review of all CIO Organization policies and procedures;
- The development of an *Incident Response Program Guide* consistent with NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*.
- Revision of the FDIC's *Data Breach Handling Guide* to incorporate policy guidance promulgated in OMB Memorandum M-16-03 to specifically address reporting and incident escalation procedures, and the roles and responsibilities of DBMT members.
- Implementation of a new incident tracking system to automate, centralize, and enhance the management and oversight of incident response and breach-related activities.
- Restrictions on employee use of removable media, except in cases approved by a division or office director for a legitimate business need where no other technical solutions are available.
- Restrictions on the use of printed documents that contain sensitive information, such as large quantities of SSNs.
- Implementation of Digital Rights Management software to protect the FDIC's most sensitive data by providing additional restrictions when that data is outside of the FDIC's network.
- Engagement of a third-party contractor to conduct an end-to-end assessment of the FDIC's IT security and privacy programs.

The OIG will continue to monitor the FDIC's progress in implementing corrective actions to strengthen its information security program.

Corporation Comments and OIG Evaluation

The CIO provided a written response, dated June 30, 2016, to a draft of this report. The response is presented in its entirety in Appendix 4. In the response, the CIO concurred with all five of the report's recommendations. In addition, the response describes planned corrective actions to address the recommendations. A summary of the Corporation's corrective actions is presented in Appendix 5. The planned actions are responsive to the recommendations, and the recommendations are resolved.

Appendix 1

Objective, Scope, and Methodology

Objective

The audit objective was to determine whether the FDIC has established key controls that provide reasonable assurance that major security incidents are identified and reported in a timely manner.

We conducted this performance audit from January through June 2016 in accordance with generally accepted government auditing standards. Except as noted in the report, our findings and conclusions are as of June 16, 2016. The standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Scope and Methodology

The scope of the audit included: (1) an assessment of the FDIC's controls related to major incidents, including internal and external (i.e., the Congress) communications, the role of the DLP tool, and the documentation of investigative activities, and (2) a detailed analysis of the FDIC's handling of an information security incident in which a departed employee copied multiple files, including business and personal information, from an FDIC computer to a personally-owned USB device (referred to in the report as the Florida Incident). We did not analyze the FDIC's handling of other incidents, including those reported by the FDIC to the Congress as major.

To achieve the audit objective, we:

- identified and reviewed relevant criteria, including FISMA; OMB Memorandum M-16-03; OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*; OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*; the Memorandum of Understanding between FDIC and FinCEN; Fin-2010-A014, *Maintaining the Confidentiality of Suspicious Activity Reports*; and GAO's *Standards for Internal Control in the Federal Government;*

- assessed relevant FDIC incident response policies, procedures, and guidance, such as the FDIC's *Data Breach Handling Guide*, Version 1.4, dated April 16, 2015; FDIC Circular 4010.3, *FDIC Enterprise Risk Management Program*; dated April 16, 2012; FDIC Circular 1360.9, *Protecting Sensitive Information*, dated April 30, 2007, and FDIC Circular 1360.12, *Reporting Computer Security Incidents*, dated June 26, 2003;

Objective, Scope, and Methodology

- gained an understanding of the FDIC's implementation of the DLP tool, most notably its use to detect the downloading of sensitive data to removable media and the level of resources dedicated to implementing the tool.

- reviewed incident investigation-related activities, records, decisions, and reports for one specific incident—FDIC Security Incident Number CINC-221387 (referred to herein as the Florida Incident). We selected this incident by first requesting from ISPS a listing of all computer security incidents that (a) occurred during the period from May 1, 2015 to January 11, 2016 and (b) involved former FDIC employees that transmitted sensitive FDIC information to removable media within 30 days of separating from the FDIC. In response to our request, ISPS provided us with a listing of 18 incidents. We judgmentally selected one of these incidents—the Florida Incident—because it appeared on the surface to have characteristics consistent with a major incident, as that term is defined in OMB Memorandum M-16-03. We reviewed the facts and circumstances of the incident to determine whether it satisfied the criteria for being designated as major; and

- interviewed FDIC officials to determine their roles, responsibilities, and perspectives related to the Florida Incident and the FDIC's incident response program as a whole. Such officials included the:

    - Former Chief Information Security Officer
    - Acting Chief Information Security Officer
    - Chief Information Officer
    - Deputy General Counsel
    - ISPS Incident Lead for the Florida Incident and other ISPS staff
    - Legal Division personnel familiar with the Florida Incident
    - RMS personnel familiar with the Florida Incident

Regarding compliance with laws and regulations, we analyzed the FDIC's compliance with relevant provisions of FISMA and OMB Memorandum M-16-03 pertaining to the identification and reporting of major incidents. In addition, we assessed the risk of fraud and abuse related to our objective in the course of evaluating audit evidence.

We performed our work at the FDIC's Headquarters offices in Washington, D.C. and at Virginia Square in Arlington, Virginia.

Appendix 2

Glossary of Terms

Term	Definition
Cyber Threat	A cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through a system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
Data Classification Standards	Data classification standards refer to protocols that describe under what circumstances a document should be marked, under what circumstances a document should no longer be considered sensitive but unclassified, and what procedures should be followed to properly safeguard or disseminate the information.
Data Loss Prevention Tool	Data loss prevention software is designed to detect and, if enabled, prevent potential data breaches by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
High Value Asset	High Value Assets refer to those assets, systems, facilities, data and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions or data used in critical Federal operations, or house unique collections of data (by size or content) making them of particular interest to criminal, politically-motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. Government.
Information Security Manager (ISM)	ISMs are located within FDIC divisions and offices and provide a business focus on information security and coordinate with the CIO Organization to ensure that security controls are in place to protect their respective division or office's information and systems. ISMs are responsible for such things as educating employees and contractors on how to properly safeguard FDIC information; ensuring that security requirements are addressed in new and enhanced systems; and promoting compliance with security policies and procedures.
Major Incident	According to OMB Memorandum M-16-03, a major incident will be characterized by a combination of the following factors: (1) involves information that is Classified, CUI proprietary, CUI Privacy, or CUI Other; and (2) is not recoverable, not recoverable within a specified amount of time, or is recoverable only with supplemental resources; and (3) has a high or medium functional impact to the mission of an agency; or (4) involves the exfiltration, modification, deletion or unauthorized access or lack of availability to information or systems within certain parameters to include either: (a) a specific threshold of number of records or users affected; or (b) any record of special importance.

Appendix 2

Glossary of Terms

Term	Definition
Personally Identifiable Information (PII)	FDIC Circular 1360.9, *Protecting Sensitive Information*, defines PII as any information about an individual maintained by the FDIC that can be used to distinguish or trace that individual's identity, such as their full name, home address, email address (non-work), telephone numbers (non-work), SSN, driver's license/state identification number, employee identification number, date and place of birth, mother's maiden name, photograph, biometric records (e.g., fingerprint, voice print), etc. This also includes, but is not limited to, education; financial information (e.g., account number, access or security code, password, personal identification number); medical information; investigation report or database; criminal or employment history or information; or any other personal information that is linked or linkable to an individual.
United States Computer Emergency Readiness Team (US-CERT)	Established in 2003, the US-CERT's mission is to protect the nation's internet infrastructure. US-CERT coordinates defense against and responses to cyber-attacks across the nation. In the event of a loss or compromise of business sensitive information and/or PII, US-CERT is responsible for notifying appropriate officials in the executive branch of the government about the breach incident; coordinating communications of the breach incident with other agencies; and for PII incidents, distributing to designated officials in the agencies and elsewhere, a monthly report identifying the number of confirmed breaches of PII and making available a public version of the report.

Appendix 3

Abbreviations and Acronyms

BSA	Bank Secrecy Act
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
CUI	Controlled Unclassified Information
DBMT	Data Breach Management Team
DIT	Division of Information Technology
DLP	Data Loss Prevention
FinCEN	Financial Crimes Enforcement Network
FISMA	Federal Information Security Modernization Act
GAO	Government Accountability Office
IRA	Incident Risk Analysis
ISM	Information Security Manager
ISPS	Information Security and Privacy Staff
IT	Information Technology
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
RMS	Division of Risk Management Supervision
SAR	Suspicious Activity Report
SSN	Social Security Number
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team

Appendix 4

Corporation Comments

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C., 20429

DATE: June 30, 2016

MEMORANDUM TO: Mark F. Mulholland
Assistant Inspector General for Audits

FROM: Lawrence Gross, Jr. /Signed/
Chief Information Officer

SUBJECT: Response to the Draft Audit Report Entitled *The FDIC's Process for Identifying and Reporting Major Incidents* (Assignment No. 2016-023)

The Federal Deposit Insurance Corporation (FDIC) has completed its review of the Office of Inspector General's (OIG) draft audit report entitled The FDIC's Process for Identifying and Reporting Major Incidents dated June 16, 2016.

We appreciate the OIG's analysis and findings and concur with the five recommendations. In retrospect, and in light of the findings in this report, we should not have considered what we believed to be mitigating factors when applying Office of Management and Budget (OMB) major incident guidelines. We have since updated our internal procedures to refer FDIC employees and contractors directly to the OMB guidelines on what constitutes a "major" incident. We believe this will be effective in ensuring proper assessment of any future incidents.

We recognize that enhancements to FDIC policies, procedures, and guidelines are necessary to further address the report findings. Also, reviews of particular information security functions are necessary to improve the FDIC's protection of sensitive information. We believe the steps we are taking to address the OIG's recommendations will strengthen the FDIC's controls over sensitive information and improve our incident handling, particularly our notification process.

Our response to the OIG's specific recommendations below is organized by recommendation and enumerates actions planned, in process, and completed to date.

Recommendation 1: The OIG recommends that the Chief Information Officer (CIO) revise the FDIC's incident response policies, procedures, and guidelines to address major incidents.

Management Decision: Concur

The OIG report notes that FDIC incident response policies, procedures, and guidelines did not address major incidents. We have begun revising our incident response policies, procedures, and guidelines in response to the audit findings. On June 13, 2016, we published an interim update to our Data Breach Handling Guide that directs the reader to the Federal Information Security Modernization Act of 2014 (FISMA) and OMB

Corporation Comments

Memorandum M-16-03 (M-16-03) to consider when external incident notification steps are required. This is an interim step that focuses appropriate members of the FDIC community on the key relevant documents relating to major incidents. We plan to make more extensive and substantive changes to the *Data Breach Handling Guide*, and will also revise FDIC Circular 1360.2 entitled *Reporting Computer Security Incidents*, including refining the roles and responsibilities for designating incidents appropriately, in line with the requirements of FISMA and M-16-03. Changes will also address escalating incidents for action, including the timeliness of decision-making and Congressional notification. In addition to ensuring our policies, procedures, and guidelines adequately address FISMA and M-16-03, we will consult applicable NIST publications to ensure all our incident handling is comprehensive and consistent with statutory and other requirements.

Corrective Action: We will revise FDIC incident response policies, procedures, and guidelines to address major incidents.

Completion Date: September 30, 2016

Recommendation 2: The OIG recommends that the CIO review the current implementation of the Data Loss Prevention (DLP) tool, including the keywords and filters used to monitor data, procedures for assessing output, and resource commitments, to determine how the tool can be better leveraged to safeguard sensitive FDIC information. As part of this effort, consider planned and ongoing efforts related to data classification standards and the identification and protection of high value assets.

Management Decision: Concur

The OIG report notes that the FDIC's deployment of the DLP tool was characterized by several weaknesses that limited the FDIC's assurance that all incidents, including major incidents, were being identified and reported. We agree that our DLP tool can be better leveraged to identify and potentially mitigate major incidents. Although the risks of harm from copying sensitive information to removable media are being lowered dramatically as we phase out the use of removable media for information transfer, it will be beneficial to review how the DLP tool can be used to improve further the FDIC's ability to monitor sensitive information beyond the screens that are currently in place. For example, it may be possible to screen for activity related to high value assets in ways that are not currently implemented. In addition to assessing how to better utilize the tool's capabilities, we will assess the processes and procedures in place for using the tool, and staffing levels, to ensure the tool is adequately leveraged. We are also evaluating Digital Rights Management (DRM) software that may complement DLP capabilities. DRM software

[1] As of June 30, 2016, with very limited exceptions, no FDIC employees or contractors are able to copy information to removable media. To the extent exceptions to this rule are allowed, there will be strong controls over the business functions requiring the exceptions.

Corporation Comments

may provide additional preventative protections that are unavailable using the DLP tool alone.

Corrective Action: We will review the current implementation of the DLP tool to determine how the tool can be better leveraged to safeguard sensitive FDIC information. In this connection, we will consider, as appropriate, data classification standards guidance in assessing DLP tool keywords and filters. We will also develop and follow a project plan that identifies any approved tasks resulting from the DLP review, and also implement DRM software as appropriate in light of the evaluation we are conducting. These activities will be carried out in conjunction with any findings and recommendations that may come out of the upcoming end-to-end assessment of the FDIC's IT security and privacy programs.

Completion Date: December 30, 2016

Recommendation 3: The OIG recommends that the CIO ensure that the revisions to the FDIC's incident response policies and procedures addressed in recommendation 1 include criteria for determining whether an incident is major consistent with FISMA and M-16-03.

Management Decision: Concur

The OIG report notes that the FDIC did not properly apply OMB guidelines in its evaluation and reporting of the Florida incident. It is important that any determination of whether an incident is major or not be made consistent with FISMA and M-16-03. As noted above, we have published an interim update to our *Data Breach Handling Guide* that directs the reader to FISMA and M-16-03 to consider when external incident notification steps are required. To ensure ongoing consistency between FDIC policy and procedure and OMB guidance, we will also review FDIC policies and procedures periodically in light of any relevant OMB revisions or other guidance obtained from OMB.

Corrective Action: We will ensure that policy and procedure revisions are clear with respect to the criteria that should be applied for determining when an incident is major consistent with FISMA and with M-16-03.

Completion Date: September 30, 2016

Recommendation 4: The OIG recommends that the CIO establish controls to ensure that future Congressional notifications of major incidents include appropriate context regarding the risks associated with those incidents and that statements of risk are supported by sufficient, appropriate evidence.

Management Decision: Concur

Corporation Comments

The OIG report notes that the FDIC Congressional notifications did not accurately portray the extent of risk associated with the incident. It is important that FDIC Congressional notifications of major incidents include appropriate context regarding the risks associated with the incidents.

Corrective Action: We will promptly establish a review process to ensure that future Congressional notifications of major incidents include appropriate context.

Completion Date: July 8, 2016

Recommendation 5: The OIG recommends that the CIO review and update, as appropriate, incident response policies, procedures, and guidelines to require that (a) documentation related to investigation activities and decision-making is properly recorded and centrally maintained, (b) IRAs [Incident Risk Analyses] contain current, accurate, and complete information throughout the investigation supported by sufficient, appropriate evidence, and (c) the underlying analyses for key decisions and discussions are adequately documented.

Management Decision: Concur

As the OIG report notes, management of incident investigative records and related documentation needs improvement. We agree that incident documentation should be managed centrally; that it should be kept current, accurate, and complete; and that it should contain the underlying analysis for key decisions and discussions.

Corrective Action: We will review and update, as appropriate, the incident response policies, procedures, and guidelines as specified in the recommendation.

Completion Date: September 30, 2016

Please contact me at (202) 898-6630, or Rack Campbell at (703) 516-1422, with any questions you may have regarding this response.

cc: James H. Angel, Jr., Deputy Director, DOF, Corporate Management Control
Roderick E. Toms, Acting CISO, Information Security & Privacy
Russell G. Pittman, Director, DIT
Steven P. Anderson, Deputy Director, DIT, Business Administration Branch
Rack D. Campbell, Supervisory IT Specialist, DIT, Audit and Internal Control
Barbara A. Ryan, Deputy to the Chairman and Chief Operating Officer, Chief of Staff

Appendix 5

Summary of the Corporation's Corrective Actions

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The FDIC will revise its incident response policies, procedures, and guidelines to address major incidents consistent with FISMA and OMB Memorandum M-16-03. The revisions will address roles and responsibilities for designating major incidents as well as escalating incidents for action, including the timeliness of decision-making and Congressional notifications.	9/30/2016	No	Yes	Open
2	The FDIC will review its current implementation of the DLP tool to determine how the tool can be better leveraged to safeguard sensitive information and identify and potentially mitigate major incidents. The review will cover processes and procedures for using the DLP tool and staffing levels. Additionally, FDIC will consider data classification standards guidance and its work to identify high value assets. Further, the FDIC will develop and follow a project plan that identifies tasks identified during the review and implement Digital Rights Management software, as appropriate, to complement DLP capabilities.	12/30/2016	No	Yes	Open
3	The FDIC will ensure that policy and procedure revisions are clear with respect to the criteria that should be applied for determining when an incident is major consistent with FISMA and OMB Memorandum M-16-03.	9/30/2016	No	Yes	Open
4	The FDIC will promptly establish a review process to ensure that future Congressional notifications of major incidents include appropriate context.	7/8/2016	No	Yes	Open

Appendix 5

Summary of the Corporation's Corrective Actions

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
5	The FDIC will review and update, as appropriate, the incident response policies, procedures, and guidelines to require that (1) incident documentation is properly recorded and centrally maintained, (2) IRAs contain current, accurate, and complete information throughout the investigation supported by sufficient, appropriate evidence, and (3) the underlying analysis for key decisions and discussions are adequately documented.	9/30/2016	No	Yes	Open

[a] Resolved – (1) Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but alternative action meets the intent of the recommendation.
(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Recommendations will be closed when (a) Corporate Management Control notifies the OIG that corrective actions are complete or (b) in the case of recommendations that the OIG determines to be particularly significant, when the OIG confirms that corrective actions have been completed and are responsive.

DOCUMENT SUBMITTED BY REPRESENTATIVE RANDY NEUGEBAUER

Transcribed Interview of an FDIC Employee

Q: And could you tell us a little bit more about the laptops? So under this new plan would it replace the desktops that employees have at the agency?

A: It's not clear. And this is one of the things that has not been thought through. Some of the questions are, "So this will replace the desktop? Do you have both? So now I have a laptop and I have to take that back and forth?"

Now, again, I'm looking at it from the security perspective. ... Our focus has been security. What is the risk of -- you know, why spend $5 million? Is this really going to help the security posture for FDIC in terms of you're spending something, what are you getting in return, from the security perspective.

There are many other things [sic] we can be doing to improve the security posture at FDIC, and this is not at the top of that list, really.

***

But this is what happens when decisions are made at the top level without including subject matter experts, folks from the divisions, from the business. And then artificial deadlines imposed by the -- July 31st they're supposed to do all of this.

DOCUMENT SUBMITTED BY REPRESENTATIVE GARY PALMER

Transcribed Interview of an FDIC Employee

Q. Just to be clear here for the record, there was a penetration into the FDIC network system generally by an outside party that was malicious, right? Correct?

A. Yes.

Q. And the FBI alerted the FDIC the appropriate people within the FDIC that this was the case, and one of the potential fixes or appropriate actions was to shut down or turn off the entire FDIC system to eradicate the intruder.

A. Yes. That's what was recommended.

Q. Okay.

A. Now, after that, it was kept I'm out of the loop, except for when Ned came into my office to tell me that this incident that Russ Pittman said: This can't get out of here, this breach information. We can't do anything to jeopardized the chairman getting when they vote getting

[...]

A. Approved for 'cause it's a

Q. A Senate approved position.

Q. Confirmed.

A. Yes.

DOCUMENT SUBMITTED BY REPRESENTATIVE BRUCE WESTERMAN

Transcribed Interview of an FDIC Employee

Q. Were those updates being provided to anyone in the chairman's office or the chairman himself?

A. Let's see. At the time, it was Roddy, Brian, myself, Martin, Chris, and Russ Pittman. The COO was later added

Q. Is that Barbara Ryan?

A. on December 1st.

Q. Barbara Ryan is the COO and chief of staff to the chairman. Is that correct?

A. Yes.

Q. Does she act as the chairman's eyes and ears in meetings like this?

A. My understanding. I don't have direct knowledge of that, but yes.