



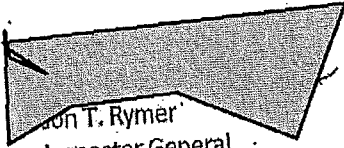
Federal Deposit Insurance Corporation
3501 N. Fairfax Drive, Arlington, VA, 22226

Office of Inspector General

Date: May 24, 2013

Memorandum To: Martin J. Gruenberg
Chairman

From:


William T. Rymer
Inspector GeneralSubject: Investigation of Division of Information Technology
Computer Security Incident

Securing government information is essential to the economic and national security interests of the United States. The FDIC possesses a huge volume of information needed to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain day-to-day functions, and protect individuals. Much of this information is highly sensitive, and some is proprietary. The FDIC employs and manages a multitude of complex systems and applications that store, process, and transmit this sensitive information. The FDIC Board of Directors entrusts responsibility for the safety and security of the FDIC's information to the Division of Information Technology (DIT).

The attached report presents the results of the FDIC OIG's investigation of DIT's handling of a serious computer security incident involving the penetration of FDIC computer systems by an advanced persistent threat (APT). DIT management officials breached their duties in their handling of this incident. As such, the Corporation was unduly subjected to increased risk, and actual, unauthorized access to and exfiltration of sensitive data. Our work suggests that there are a number of matters that warrant your attention:

As our report explains in more detail, once aware of the security incident, DIT chose to keep the preponderance of related information and decision-making within its own Division. The decision to do so was grounded in DIT's assessment that the incident was an "operational" matter. This assessment was, and remains today, fundamentally flawed and resulted in the FDIC not taking actions that should have begun at the outset in August 2011. Incidents involving APTs occur with some frequency as the government and private industry find themselves as targets of a wide variety of malicious actors. However frequent, incidents involving APTs are highly significant events that should trigger prompt disclosures to multiple parties outside of the organization under attack, as well as an enterprise-level assessment of the consequences of the attack within the organization itself.

In order to implement the flawed assessment that the presence of significant and widespread APT activity within the FDIC's network was an "operational" matter, DIT managers elected not to report, or to underreport, information regarding the incident over an extended period of time. Specifically:

- DIT did not fully inform you, other Board Members, and the Chief Risk Officer of the severity and magnitude of the intrusion. The only briefing that you received minimized the extent of the penetration of the FDIC's system, while emphasizing that DIT had the situation under control. As a result, you and others who are entrusted with ultimate governance and risk management responsibilities at the FDIC lacked critical knowledge of which to take responsive actions that you may have deemed appropriate under the circumstances. You were not updated on information subsequently developed by DIT, or the progress and efficacy of DIT's mitigation efforts, which continue through the date of this report.
- DIT violated its own policies and procedures for handling computer security incidents and did so deliberately. Established policy for reporting computer security incidents to the FDIC's CSIRT were not followed and forming an incident response team comprised of a broad representation of FDIC officials from multiple FDIC Divisions and Offices never occurred. As such, procedures designed to ensure an enterprise-level assessment of the incident and DIT's response to it, including procedures designed to protect and safeguard personally identifiable information, were circumvented.
- Counterparties to Interconnection Sensitivity Agreements with the FDIC—that is, other federal financial regulators, government agencies, financial institutions, and private-sector service providers—were not notified of the computer security incident. Under these agreements, counterparties have the right to assess for themselves the potential impact that penetration of the FDIC's systems could have on them or their data. Such an analysis cannot be performed unilaterally by the FDIC. In failing to notify these parties, DIT managers may have exposed the FDIC to significant risk.
- In violation of FDIC policies and procedures and federal guidelines, until May 2013, DIT management chose not to report the security incident in any meaningful way to US CERT, the central national authority responsible for tracking, analyzing, and coordinating responses to computer security incidents, including APTs that attack US government systems. As such, US CERT did not have the benefit of FDIC data to incorporate in US CERT's efforts to protect the nation's cyber security and manage cyber risks. As evidenced in recent press coverage, foreign nations are engaging in sophisticated attempts to gain access to military, financial, and other confidential or proprietary data. As outlined in government-wide guidance, information related to the infiltration at the FDIC should have been fully disclosed to US CERT in a timely manner, and updated on a continuing basis.
- Finally, with respect to auditors from the Government Accountability Office (GAO) and the OIG, the non-disclosures or misstatements on the part of DIT call into question the underlying factual basis for opinions and conclusions that the GAO and OIG reached in their respective audit work—namely GAO's financial statement audit work and the OIG's work in 2011 and

2012 pursuant to the Federal Information Security Management Act (FISMA) of 2002. At a minimum, DIT's behavior necessitated significant additional work on the part of both sets of auditors as they sought to determine the effects of non-disclosures on their audit products long after these products had been completed. DIT management's behavior also changed the dynamic of the relationship between the auditors and the auditee in ways that are not yet fully understood. Much of audit work is based on a trust relationship and once that trust is violated, the relationship may be irreparably damaged.

On May 16, 2013, the FDIC filed an updated notice with US CERT of the security incident, with information that should have been in the initial August 2011 filing. This information is required to be filed within one hour of the detection of the incident but was provided more than 20 months later. The notice suggests that it "encapsulates multiple events that had been previously reported." Based on our review, the relevant events were not reported, or were reported in such a manner so as to be meaningless. In addition to the matters specifically addressed in our report, we believe that your attention to management's continuing approach to the handling of the security incident is warranted.

The OIG is monitoring the actions that DIT is taking related to handling computer security threats. We will be evaluating those actions in more detail as part of our 2013 FISMA audit. Given the significance of the APT itself and the results of our investigation, I will be notifying appropriate Congressional Committees of this matter as I am required to do under the Inspector General Act. In the interim, we request that you inform us of any actions that you take to address the findings in our attached investigative report.



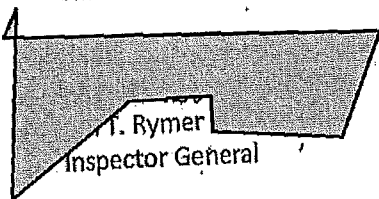
Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, Virginia 22226

Office of Inspector General

Date: May 24, 2013

Memorandum To: Martin J. Gruenberg
Chairman

From:



J. Rymer
Inspector General

Subject: Investigation of Division of Information Technology
Computer Security Incident

The security of government information is important to the economic and national security interests of the United States. The FDIC has a large volume of information it needs to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions and protect individuals. The FDIC in carrying out its wide range of responsibilities, employs and manages a complex variety of systems and applications that store, process and transmit this sensitive information. The FDIC Board of Directors has entrusted the Division of Information Technology (DIT) with the responsibility of making sure that information is safe and secure.

In October 2010, DIT became aware that an FDIC employee's desktop computer had been compromised by an advanced persistent threat¹ (APT). An APT presents challenges that are distinct from traditional security risks in that the threat is long-term, sophisticated, and targeted to a specific organization or entity. DIT executed remediation steps in an attempt to eradicate the compromise. In August 2011, DIT was alerted by a third party—the Federal Bureau of Investigation (FBI)—to network activity indicating another potential security incident involving an APT. DIT found in April 2013 that the 2010 and 2011 incidents were related attempts by the same APT.

DIT has subsequently determined that the APT penetrated over 90 workstations or servers with specialized tools that ultimately allowed the creation of valid administrator accounts providing full access to the FDIC's Windows environment. Approximately 90 percent of the FDIC's information technology activities are conducted in Windows. DIT also discovered evidence that the APT had exported data from FDIC machines to servers outside the FDIC network. Twelve of the infected computers were those of FDIC executives, including the former FDIC Chairman, Director and Deputy

¹ The National Institute of Standards and Technology defines an APT as an adversary that possesses significant levels of expertise; creates opportunities to achieve its objectives by using multiple attack vectors; and establishes footholds within the IT infrastructure of targeted organizations to exfiltrate information; undermine critical aspects of a mission or program; and position itself to carry out these objectives in the future.

Director of the Office of International Affairs (OIA), former General Counsel, and Chief Economist. (Attachment 1 presents a listing and brief explanation of the compromised workstations or servers.)

OIG Investigation

In March 2013, the FDIC Office of Inspector General (OIG) received information that caused the OIG to ask DIT management about DIT's notification and handling of the security incident. The information that we initially received on this matter raised serious concerns as to how it was managed and communicated within and outside the Corporation. Accordingly, the OIG initiated an investigation to understand the events surrounding the security incident.

During the period from April 1, 2013 through May 22, 2013, we interviewed 22 DIT employees, including Rus Pittman, the DIT Director and Chief Information Officer (CIO) and Chief Privacy Officer; [REDACTED], DIT Deputy Director and Chief Information Security Officer (CISO); Roderick Toms, Assistant DIT Director, Security Protection Engineering Section; FDIC Chairman, Martin Gruenberg; members of the FDIC Chairman's staff; senior FDIC officials; Government Accountability Office (GAO) representatives; and Special Agents from the FBI to determine steps taken, timeframes, and notifications regarding the incident. In conducting our work, we reviewed DIT's communications with FDIC senior officials and others, including e-mail communications; and applicable policies, procedures, and mandatory notification requirements. We also considered the disclosures that DIT made to GAO and OIG auditors as these auditors were conducting audit work related to the financial statements of the FDIC and the Federal Information Security Management Act of 2002 (FISMA), respectively.

The following sections of this report present the results of our investigation. We first include a chronology of key events. We then discuss DIT's (1) communication of the computer security incident to the FDIC Chairman and other senior officials; (2) adherence to certain FDIC and government-wide policies, procedures, and guidelines for dealing with computer security incidents; (3) notifications to parties external to the FDIC; and (4) disclosures to GAO and OIG auditors.

Chronology of Key Events

October 2010

A former FDIC OIG Special Agent, now working in a different agency, contacts [REDACTED], FDIC OIG Special Agent in Charge (SAC) of the Electronic Crimes Unit concerning a computer security incident involving the FDIC. While performing weekend reserve duties conducting cyber investigations, he discovered an IP address belonging to an FDIC workstation that was beaconing out to a known malicious command and control server outside of the FDIC network. SAC [REDACTED] informs [REDACTED] Senior IT Security Specialist, FDIC.

October 19, 2010

The former Special Agent, SAC [REDACTED] and [REDACTED] meet with Assistant Inspector General for Investigations Matt Alessandrino to discuss the incident.

- October 28, 2010 SAC [redacted] go to the United States Computer Emergency Readiness Team (US CERT) in Arlington, Virginia. [redacted] provides US CERT a copy of the malware found on the infiltrated machine.
- November 18, 2010 SAC [redacted] attend a regularly scheduled cyber working group meeting. [redacted] provides a copy of the image of the compromised machine to the group for analysis. The head of the group indicates that another government agency is at the late stages of a broader investigation to which the information pertained. DIT plans to continue to look for other compromised computers and perform needed remediation. The OIG decides not to investigate because of the risk of disrupting another agency's investigation.
- August 2011 [redacted] invites SAC [redacted] to a meeting with the FBI. Special Agent [redacted], FBI, had contacted [redacted] to set up a meeting to discuss a computer security incident involving the FDIC network.
- August 10, 2011 Special Agent [redacted] meets with [redacted] and SAC [redacted] and informs them that a host computer known to support malicious activity has downloaded files to an FDIC IP address.
- August 2011 DIT initiates an investigation of the FDIC systems communicating with the command and control server. [redacted] indicates [redacted] will keep SAC [redacted] informed. SAC [redacted] is subsequently invited to another meeting but cannot attend. He receives no other information about the incident until March 2013.
- August 26, 2011 Mr. Pittman and [redacted] brief the then-Acting Chairman, Chief of Staff, former Chief of Staff, and Chief Risk Officer on the security incident.
- August 31, 2011 A DIT security official directs the FDIC's Computer Security Incident Response Team (CSIRT) to open a new "general virus incident" and report the incident to US CERT as a Category 3 Event (Virus).
- October-November 2011 DIT determines that the risk associated with the security incident is significant enough to warrant a number of short-, medium-, and long-term actions, including the rebuilding of several compromised servers and workstations, requiring a shutdown of the network, and the resetting of passwords. The rebuilding event is originally planned for the 3-day Columbus holiday weekend in October 2011, but DIT postpones the event to the 3-day Veteran's Day weekend in November 2011. (Note: Network shutdown does not take place.)

- Summer/Fall 2012** DIT submits a mid-term budget request for \$250,000 to contract with Mandiant Corporation, a cyber-security company that assists organizations in dealing with targeted cyber-attacks on their networks. [REDACTED] has several phone conversations with Mandiant to discuss work needed and contractual issues.
- January 18, 2013** The FDIC executes a contract with the Mandiant with an effective date of December 21, 2012. The objective of the contract is to assist the FDIC in responding to a suspected security incident and to help identify and investigate remedial efforts. The contract had been proposed in mid-2012, but according to a DIT official, was delayed by contracting and budgeting issues.
- March 25, 2013** The Inspector General meets with Mr. Pittman and informs Mr. Pittman that the OIG has independently learned that the FDIC has been subject to a sophisticated network compromise that began in 2010.
- March 26, 2013** The Inspector General and certain senior OIG staff meet with Mr. Pittman, [REDACTED] and Mr. Toms to discuss the network compromise, including DIT notifications during the computer security incident. [REDACTED] states that the OIG and GAO were told of the events. Further, according to Mr. Pittman, the Chairman and one other Board member had been briefed, and the incident was contained.
- March 26, 2013** The FDIC OIG initiates an investigation of events surrounding the incident.
- April 2, 2013** DIT learns from Mandiant that the October 2010 and the August 2011 incidents involve the same APT.

Communications with the FDIC Chairman and Other Senior Officials

As outlined in the FDIC's policy for reporting computer security incidents, CSIRT has an obligation to evaluate the seriousness of computer security incidents and inform FDIC senior management and the OIG within 24 hours. Mr. Pittman told the OIG on March 26, 2013, that the Chairman and senior staff were aware of the incident and that the incident had been contained. As part of our investigation, we interviewed the Chairman; his Chief of Staff, Barbara Ryan; staff of other FDIC Board Members; the Chief Financial Officer; and the Chief Risk Officer to determine their level of awareness of the computer security incident. We learned that the Chairman and senior management were not aware of the scope or severity of the incident and were not kept apprised of its ongoing nature.

On August 26, 2011, the Chairman's staff received a briefing from Mr. Pittman and [REDACTED] concerning the computer security incident. In the materials prepared for the briefing, DIT mentions that it is "addressing a malware infection...that is extremely professional and well crafted." Materials indicate that DIT has identified 78 computers that were compromised (i.e., 12 servers, 49 desktops, 15 laptops; and 2 e-copiers) and multiple data exfiltrations from the FDIC's network. The

briefing materials listed 12 executives, whose computers were compromised; including: the former Chairman, Director and Deputy Director of OIA, former General Counsel, Chief Financial Officer, and Chief Economist. Those attending the August 26, 2011 meeting stated that not all of this information was communicated by DIT during that meeting.

In an interview, Chairman Gruenberg advised that Mr. Pittman did the majority of the presentation. The Chairman recalls receiving an article from Vanity Fair magazine and a 2-page summary that may have been collected at the end of the briefing. He indicated that Mr. Pittman's briefing was a general summary of a security issue that DIT had been notified of by the FBI. Mr. Pittman indicated that DIT was working with the FBI to address an intrusion attempt by a foreign entity. According to the Chairman, the tone of the briefing suggested the matter was a routine computer security event that is common throughout the federal government. Mr. Pittman indicated that DIT was aware of the threat, identified the affected computers, contained the problem, and had implemented safeguards and procedures to address the security concerns. The Chairman was unaware of the earlier possibility of shutting down the FDIC computer systems or service or the hiring of contractors to assist with the matter.

In an interview, Ms. Ryan stated that the August 26, 2011 meeting had lasted about an hour. She indicated that Mr. Pittman's briefing involved a Vanity Fair article about hacking titled "Enter the Cyber-Dragon" which he used to explain how common the incident was among other organizations. He explained there were workstations affected but DIT had controls in place to handle the issue and was working with the FBI. Ms. Ryan also stated that Mr. Pittman discussed how 15 megabytes of data had been exfiltrated from the former Chief of Staff's computer. Mr. Pittman explained that the 15 megabytes of data had been exported, but because the data had been encrypted before export, DIT could not identify any of the data that had been lost.² Ms. Ryan recalled Mr. Pittman saying that the computer security incident was contained. She stated that Mr. Pittman and [REDACTED] tone lacked a sense of urgency about the computer security incident. Ms. Ryan was unaware that DIT had planned to shut the network down for 3 days in October or November 2011 in order to implement certain remedial actions. She was also unaware until just recently that DIT had attempted to contract with Mandiant to assist the FDIC in dealing with targeted cyber-attacks on the FDIC network.

Both the Chairman and Ms. Ryan indicated that the August 26, 2011 briefing was the last briefing that the Chairman's Office received from DIT concerning the computer security incident. Both further noted it was not brought up again until March 2013 when the FDIC OIG notified the Chairman and his staff about possible reporting issues concerning the intrusion in connection with the OIG's FISMA reporting for 2011 and 2012.

The FDIC's Chief Risk Officer, Steve Quick, attended the August 26, 2011 briefing given by Mr. Pittman and [REDACTED]. Mr. Quick started working at the FDIC in mid-August 2011. Mr. Quick stated that Mr. Pittman did most of the speaking and he (Mr. Pittman) explained how the FDIC had been attacked by hackers that left some code on several of the machines. Mr. Pittman handed out an article to everyone at the briefing titled "Enter the Cyber-Dragon" from Vanity Fair.

² We have subsequently learned that some of the information had not been encrypted, but no efforts had been made to determine what type of information this was, notwithstanding that the file names appear to be sensitive.

Mr. Quick stated Mr. Pittman may have handed out something else during the briefing but he (Mr. Quick) does not remember. He was shown briefing material prepared by Mr. Pittman, but did not recall seeing such a document at the meeting.

Mr. Quick stated that Mr. Pittman said DIT had identified the code and the external server involved in the incident and DIT had stopped it. Mr. Pittman told the group that DIT had the intrusion well controlled and also mentioned that more than 10 FDIC servers had been infected. Mr. Pittman said that the code the hackers left behind would beacon out to servers outside of the FDIC. Mr. Pittman said DIT had identified the hacker's IP addresses and because of DIT's early detection and remediation, there was not much damage to the FDIC network. Mr. Pittman said he would keep everyone informed of any new developments involving the intrusion. Mr. Quick did not receive another computer intrusion briefing from anyone in DIT until March 2013.

Mr. Quick stated that Mr. Pittman's style is to always express confidence and that he gave everyone the impression at the briefing he was on top of the situation. Mr. Quick stated that he got the impression from the August 26, 2011 briefing that this kind of event happens all the time and DIT was controlling the situation. Mr. Quick stated that he does not remember Mr. Pittman or [REDACTED] mentioning anything about data being exfiltrated by the hackers during the briefing.

Mr. Quick also stated that he attended a DIT meeting in October 2012 about cellular devices and overseas travel but the computer security incident was only briefly mentioned. Mr. Quick vaguely remembers being told something about a network shutdown in the fall of 2011 and never associated it with the computer security incident. Mr. Quick was not aware that DIT had contracted with Mandiant, until just recently.

In April 2013, the Chairman's staff received multiple, separate briefings from DIT and the OIG about the computer security incident. It was from the OIG that the Chairman's Office became aware that the incident may still not be contained.³

In another interview, the FDIC Chief Financial Officer, Steve App, stated that in August 2011, Rus Pittman told him that the FBI had recently met with [REDACTED] and informed him that there was a security incident at the FDIC. Mr. App described it as an email phishing event. He was aware of the August 26, 2011 briefing but did not attend. He was told by Mr. Pittman that the intrusion was under control and that contractors were helping out. Mr. App mentioned several times that the same type of event was happening all over town to other organizations. He stated he was not aware of what the intrusion was or how significant it was. He stated there were some processes that DIT should have followed during the incident such as a Privacy Incident Response Team (as discussed in the next section of this report) and CSIRT. He did not know whether the Chairman and his staff were aware of the ongoing threat related to the intrusion. He was aware that DIT had planned a 3-day remediation that involved shutting down the network and thought it was a routine event. He thought the incident was contained and still thinks it is contained.

Mr. Pittman stated in an interview that he thought the Chairman understood the issue. He did not inform the Chairman of the planned 3-day network shut-down, but stated that he had informed the

³ We have become aware that Mandiant has recommended that DIT take specific additional steps and follow additional best practices.

Chairman's office that some servers needed to be worked on due to the intrusion. He stated that he did not think he told the Chairman's office about contracting with Mandiant. [REDACTED] stated in an interview that he had given Mr. Pittman bullet points for the Chairman's first briefing about the security incident. He stated that he did not remember telling the Chairman's office that the computer security incident was contained. [REDACTED] also stated that he and Mr. Pittman had decided to keep information on "very close hold."

With respect to other Board Members—that is, the FDIC's internal Board Members—based on interviews with their Deputies, the Directors either had no knowledge or had never been informed of the severity of the computer security incident.

We understand from DIT that it has briefed a number of senior FDIC and GAO officials subsequent to our March 26, 2013 meeting with DIT; however, it was not within the scope of our investigation to confirm all such meetings.

FDIC Policies and Procedures

The FDIC provides policy and guidance on responding to computer security incidents, breaches of sensitive information, and breaches of Personally Identifiable Information (PII). (See Attachment 2 for a listing of applicable documents.) DIT management chose not to follow several FDIC policies and procedures related to such incidents.

FDIC policy defines some key terms that are relevant to our report, as follows:

- A **computer security incident** is "an event that threatens the security of FDIC Automated Information Systems, including FDIC's computers, mainframe, networks, software and associated equipment, and information stored or transmitted using that equipment." As also stated in the policy, Automated Information Systems may be threatened by, for example, attempts by unauthorized individuals to gain access to the systems or any attempt to gain access to FDIC data when not authorized to view it.
- **Sensitive information** is "any information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of FDIC in carrying out its programs or the privacy to which individuals are entitled."
- **PII** is "any information about an individual maintained by the FDIC which can be used to distinguish or trace that individual's identity."

A key procedure repeated in FDIC policies is the notification and involvement of DIT's CSIRT. All users of FDIC computer systems are required to report suspected computer security incidents to CSIRT, which will investigate, track, and resolve all reported security incidents and report security incidents affecting general support systems and major applications to the CIO and FDIC management officials responsible for the security of FDIC resources. CSIRT is a component of the DIT Information Security Staff, operates under the authority of the CIO, and is authorized to address computer security incidents that occur, or threaten to occur, at the FDIC.

With respect to sensitive information, once a CSIRT investigation has been completed, and it is determined that no breach of sensitive information has occurred, the CIO or CISO will request that

CSIRT close the incident. Any other determination requires the convening of a management Incident Response Team (IRT) to assess and respond to the breach of sensitive information and discuss further actions. As for a breach of PII, a Privacy Incident Response Team (PIRT) would be assembled. Both the IRT and the PIRT consist of a diverse group of senior FDIC officials: the CIO, CISO, representatives from the Legal Division, OIG, Office of Legislative Affairs, Office of Communications, Office of the Ombudsman, Executive Office, and Division Information Security Managers. The PIRT also includes the FDIC's Privacy Program Manager. One purpose that diverse representation on the IRT and PIRT serves is to ensure broad consideration of enterprise-level risks attendant on the compromise of data.

Once convened, the IRTs are required to assess the data submitted by CSIRT and determine the appropriate course of action within 24 hours of the breach notification. However, if data analysis requires additional time to complete, the Response Team may extend the 24-hour timeframe. The procedures for the IRT and PIRT call for both teams to engage in a series of sequential steps, including determining the nature of the loss and conducting a risk assessment, determining potential impact and mitigation measures, conducting breach notifications, and completing mitigation activities and lessons learned. FDIC procedures for responding to sensitive information or PII breaches state that an effective and quick response in the event of a breach is critical to efforts to prevent or minimize any consequent harm.

With respect to the August 2011 APT, our investigation determined that DIT security officials did not comply with DIT "Circular 1360.12 (June 2003) – Reporting Computer Security Incidents." Specifically, notification was not made to CSIRT until 21 days after the discovery of the incident, rather than when it was identified, as required in the circular. In addition, when CSIRT was notified, the incident was reported as a general virus incident. Also, [REDACTED] informed CSIRT that no further information about the incident would be provided until the incident was resolved. He emailed instructions to CSIRT, as follows: "Can you please open up a new Virus incident for me - I'll be the point of contact for this incident—Just label the incident as a general virus incident called: 'Knock Knock.' This incident will be handled directly by me—Forensic review and follow up. The incident MUST remain open until you receive an email from me to close. I will not be able to provide you any further info. Note: Please report this incident to US-CERT."

Further, DIT management did not follow Circular 1360.9 – Protecting Sensitive Information (April 2007) and Procedures for Responding to Breach of Sensitive Information (February 2011 and updated in September 2012) after it was determined that potentially sensitive information and PII was likely accessed and exfiltrated from the FDIC's network.

The decision not to follow the circular and related provisions was crucial because the event met the suspected computer security incident criteria and PII was involved, as evidenced by the fact that at least one server known to contain PII had been compromised.⁴ Because these policies were not followed and sensitive information/PII procedures were not invoked, neither an IRT nor a PIRT was formed. Our investigation also revealed that as of the date of his interview in April 2013, the FDIC's Privacy Program Manager, who is a key member of a PIRT, was unaware of any on-going high-level intrusion at the FDIC.

⁴ DIT had the name of the server in August 2011 but [REDACTED] did not notify the affected office until April 1, 2013.

In interviews, Mr. Pittman and [REDACTED] stated they did not believe that a PIRT was necessary for this computer security incident. Mr. Pittman stated that he was not aware if a PIRT had been formed for the computer security incident, nor was he aware it was his responsibility to report PII loss or create a PIRT. Mr. Pittman also stated it did not occur to him to create a PIRT because he could not prove what data was extracted from the FDIC, and that PIRTs are expensive, time-consuming tasks. [REDACTED] stated that he did not form a PIRT because there was no evidence of any PII being exfiltrated. According to [REDACTED] because DIT did not know what data was lost, there was no way to rectify the situation.

United States Computer Emergency Readiness Team (US CERT)

Among CSIRT's responsibilities is to notify the Department of Homeland Security's US CERT within one hour of a computer incident. US CERT leads efforts to improve the nation's cyber-security posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. Through its 24x7 operations center, US CERT accepts, triages, and collaboratively responds to incidents; provides technical assistance to information system operators; and disseminates timely notifications regarding current and potential security threats and vulnerabilities.

US CERT defines a computer incident as follows:

"A computer incident within the Federal Government as defined by the National Institute of Standards and Technology Special Publication 800-61 is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices."

"Attempts (either failed or successful) to gain unauthorized access to a system or its data..."

Federal Incident Reporting Guidelines (which are posted on US CERT's Web site) state that:

- Agency incident reports should include a description of the incident and as much information as possible about such things as the incident's date and time, source, operating system, system function, method used to identify the incident, resolution, etc.
- Incident reporting should not be delayed to gain additional information.
- It is not always feasible to gather all of the information prior to reporting. Accordingly, incident response teams should continue to report information as it is collected.
- Category 3 Malicious Code incidents should be reported daily but within 1 hour of discovery/detection if they are widespread across the agency.
- Category 1 Unauthorized Access incidents should be reported within 1 hour of discovery/detection. In this category, an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.

The individuals responsible for the filing of an incident ticket with CSIRT and subsequent US CERT notifications all had different recollections. In an interview, [REDACTED] stated that he did not

remember whether or not he told Roderick Toms, Assistant Director, to tell the CSIRT staff to not create additional CSIRT tickets. In his interview, Mr. Toms stated that on August 31, 2011, [REDACTED] Senior IT Specialist, DIT, had opened up the shell ticket called "knock knock" in CSIRT to report the incident and also reported the incident to US CERT. Mr. Toms stated that US CERT was not notified within an hour of the incident as required by policy and no further updating or reporting was made to US CERT. Mr. Toms stated that the CSIRT ticket was a shell ticket which means it did not contain much information about the incident. [REDACTED] stated that Mr. Toms and [REDACTED] CISO, instructed him [REDACTED] not to create CSIRT tickets. [REDACTED] stated that he created the shell CSIRT ticket named "knock knock" only to protect himself.

In any case, a "shell ticket" was created and the event was reported to US CERT on August 31, 2011 as a Category 3 Event (Virus). The entire report said: "FDIC CSIRT is writing to report that an FDIC machine is potentially virus-infected. The machine is in the process of being analyzed." The "shell ticket" was untimely—21 days after the meeting with the FBI. At that time, and as evidenced by DIT's reference to a malware infection that was "extremely professional and well-crafted," DIT knew it was dealing with an APT and that 78 machines—rather than one machine—were involved. As noted earlier, 12 of the 78 compromised machines were those of senior-most FDIC executives. With the available information at that time, the filing should have been a more serious Category 1 unauthorized access incident.

DIT management provided the OIG numerous reasons for DIT's using a shell ticket, including need-to-know concerns and a lack of confidence in the confidentiality of the FDIC CSIRT incident database with respect to the APT. Although the original shell ticket was reported to US CERT, the ticket was not updated, as required by US CERT, until May 16, 2013, when the OIG brought the matter to management's attention and advised DIT to do so.

In an interview, Mr. Pittman stated that [REDACTED] had told him (Mr. Pittman) that all CSIRT and US CERT notifications were being done correctly and in a timely manner. Mr. Pittman stated that he was unaware that the appropriate CSIRT notifications were not being completed as required; however, he stated it is not part of his job description to get involved with CSIRT notifications.

Interconnection Security Agreements

DIT currently has 17 Interconnection Security Agreements (ISAs) or Memorandums of Agreement with other federal financial regulators, agencies, major financial institutions, and private-sector service providers. Most of these agreements were signed by [REDACTED] as the FDIC's CISO. Others were signed by Mr. Pittman or the former CIO. ISAs govern the relationships between the FDIC and other organizations that interconnect FDIC IT systems with partner systems for the purpose of sharing information. Although the exact language varies, all of these agreements have clauses requiring notification to the other party when a "security incident" is discovered.

As an example, the incident notification language in one such agreement states:

"Security incidents: Technical staff will, as soon as commercially reasonable or within 48 hours, notify their designated counterparts by telephone or e-mail when a security incident(s) is detected, so the other party may take steps to determine

whether its system has been compromised and to take appropriate security precautions. The system owner will receive formal notification in writing within five (5) business days after detection of the incident(s)."

During a recent briefing, Mr. Pittman and [REDACTED] were asked about the ISAs, and they could not recall the number of ISAs, who signed them, or any notification requirements. DIT has never made a notification to any ISA partner regarding the APT.

[REDACTED] stated there was no intention not to conduct ISA notifications after the breach; it was an oversight on their part. Mr. Pittman stated that it was [REDACTED] responsibility to make ISA notifications. Mr. Pittman also stated that the ISA policies needed to be modified and DIT was in the process of working with the FDIC Legal Division on the issue.

Disclosure to the GAO and OIG Auditors

During the March 26, 2013 meeting with OIG executives, [REDACTED] stated that the both GAO and OIG auditors were told of the incident. He said that GAO's auditors performing the 2012/2011 audits of the financial statements had been briefed on the APT. However, we learned that DIT officials did not disclose the activities or existence of the APT to GAO auditors responsible for conducting the 2012/2011 and 2011/2010 audits of the financial statements of the FDIC. As part of these audits, GAO assesses the effectiveness of the FDIC's information security controls over key financial systems, data, and networks. Accordingly, understanding the potential risk of the APT relative to the integrity of the financial statements was relevant to GAO's audit work.

Shortly after the March 26, 2013 meeting, the OIG spoke with the GAO auditors involved in the financial statement audit work, who informed the OIG that they had not heard about the incident until the OIG brought it to their attention. We interviewed an Assistant Director from GAO's Information Technology team who confirmed that he and his team were unaware of the compromised systems at the FDIC until March 26, 2013 when Mark Mulholland, Assistant Inspector General for Audits, called him. The GAO representative stated that [REDACTED] may have had a brief off-line conversation with a Junior staff member but there was no formal notification. The GAO representative stated he was not sure if there is an obligation to inform GAO but GAO would have preferred to know. GAO subsequently requested information about the compromises and the systems affected to see if the financial statement audit would be impacted.

We learned that GAO undertook a month-long independent review of the matter to determine what impact, if any, the events would have on the rendering of their financial statement audit opinion. The review included detailed requests for information and documentation, interviews, and briefings. GAO concluded there was not an impact on the financial statement audit opinion or on the internal controls over financial reporting. However, at the FDIC Audit Committee meeting on May 23, 2013, GAO representatives expressed ongoing concern about internal controls, indicating that the incident raised questions about policies and procedures, "tone at the top," and communications with auditors, and that management representations need to present the full picture.

Further, DIT officials did not disclose the APT to the OIG auditors responsible for conducting the 2011 or 2012 information security program evaluations required by FISMA. FISMA requires each federal agency to categorize their Information assets in accordance with standards established by the National Institute of Standards and Technology (NIST). The security categories are based on the potential impact on an organization should certain events occur that jeopardize the information systems the organization needs to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions and protect individuals. The Act also requires each agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The OIG's annual evaluations included an assessment of (among other things) the effectiveness of the FDIC's Information security risk management program and incident response and reporting capability. As such, the APT was directly related to the scope of the evaluations.

With respect to the 2012 FISMA evaluation, during the period April 2012 through September 2012, the OIG auditors participated in monthly status meetings, held 37 scheduled meetings and briefings, and exchanged numerous emails and phone calls with DIT security staff and managers to discuss security risks, program controls, and practices at the FDIC. The auditors also made 267 requests for information during the evaluation. Further, between February 2012 and March 2012, the auditors participated in 2 meetings and made 13 requests for information related to the FDIC's network perimeter security during a survey of the FDIC's Network Boundary Controls that supported the 2012 FISMA evaluation. One of these requests, which was directed to [REDACTED] in March 2012, asked for a description of the sources, targeted devices, goals, and potential damage associated with the three most prevalent types of network attacks seen in the prior 6 months. Each of the meetings, briefings, and information requests described above presented an opportunity to disclose the ongoing compromises related to the APT.

While DIT officials did not indicate that an APT was occurring at the FDIC, the CISO made references in various communications with the auditors during 2012 to general concerns he had about various IT security threats, such as non-APTs, APTs, top Internet abusers, e-mail spoofers claiming to represent the FDIC, country-to-country attacks, malware, etc. We would note that at the March 26, 2013 meeting with OIG Executives [REDACTED] stated that he had verbally informed Mr. Mulholland of the computer security event after an audit meeting at some time in the past. Mr. Mulholland said he was not aware of the event and that [REDACTED] statement was inaccurate.

In addition, the CIO's 2012 FISMA report—which was transmitted to the OMB Director, the Comptroller General of the United States, and various Congressional parties in November 2012—contained the following question and response:

Question. Provide the percentage of incidents that have been detected and attributed to successful phishing attacks. Please provide a Comment to describe any innovative and effective ways your organization has found to address these attacks.

Response. 0%. Comment: Agency has experienced no successful phishing attacks during the reporting period. Agency uses a 3rd party (Phishme.com) to create and

deliver fake phishing messages to the user community to educate them on the dangers of phishing.

The answer to the question is incorrect. DIT detected numerous security incidents during 2011, and 2012 that were attributed to one or more successful phishing attacks (which were the source of the APT).

In later interviews that the OIG conducted, Mr. Pittman and [REDACTED] stated that they had no intention of not informing the FDIC OIG of the incidents. Mr. Pittman stated that he did not inform the OIG and that it was a "blind spot." [REDACTED] referred to it as "an oversight." Mr. Pittman stated that it did not occur to him that the OIG did not know about the incident and that he believed either [REDACTED] or the Chairman's Office would have informed the OIG.

The OIG is planning a number of actions to address the fact that we were not made aware of the nature, scope, and risk of the APT and the entirety of actions being planned or taken to remediate it as we conducted our 2011 and 2012 FISMA work. Those actions—consistent with Government Auditing Standards—involve (1) advising the Chairman that we did not have sufficient, appropriate evidence on which to base certain findings and conclusions in our 2011 and 2012 FISMA audit reports; (2) performing expanded audit procedures in certain areas of the FDIC's information security program as part of the 2013 FISMA audit, particularly as it relates to the roles, responsibilities, policies, and procedures for resolving and reporting computer security incidents; and (3) notifying internal and external users of the report that those prior reports may not be reliable.

Evidence of Compromise

Over 90 workstations or servers were verified as compromised.

◆ Workstations including

- [redacted] former Chairman
- [redacted] Deputy Director OIA
- [redacted] Director OIA
- [redacted] former Chief of Staff
- [redacted] former General Counsel
- [redacted] Chief Financial Officer
- [redacted] Chief Economist
- [redacted] Associate Director, Division of Insurance and Research
- [redacted] Senior Advisor OIA
- [redacted] Deputy Director, Division of Risk Management Supervision
- [redacted] Senior Counsel, Legal Division
- [redacted] former Deputy to the Chairman

◆ E-copy (Printer/Scanner - [redacted])

- Multi-purpose scanner, copier, printing device with a [redacted] operating system computer attached. Commonly targeted by attackers for multiple reasons, including operating system vulnerabilities from [redacted] delayed patching due to proprietary software, access to all printed/scanned/copied documents, good place to hide and wait to capture administrative credentials.

◆ OIG Resource Server

- Server includes the personal network drives [redacted] of OIG personnel and contains significant amount of Sensitive Information, Personally Identifiable Information (PII), and Personal Healthcare Information.

◆ Exchange Servers

- Email Servers that process and store email.

◆ [redacted] Servers

- Remote access to applications and services not installed on the local machine.

◆ Remote Access Servers

- Authenticates users and facilitates access to FDIC network and applications including [redacted]

◆ Safeword Token Servers

- Processes [redacted] to remote access servers.

◆ **Domain Controller (Server)**

- A domain controller is the centerpiece of the [redacted] service. It authenticates users, stores user account information, and enforces security policy for a Windows domain.

◆ **Local System Accounts**

- The Local System account is a predefined local account. It has extensive privileges on the local computer, and acts as the computer on the network. [redacted] the [redacted] these accounts have access to most system objects.

Attachment 2

Documents Related to Computer Security Incidents


- (1) Circular 1360.12 – Reporting Computer Security Incidents (June 2003)
- (2) Circular 1360.9 – Protecting Sensitive Information (April 2007)
- (3) Procedures for Responding to Breach of Sensitive Information (February 2011 and updated in September 2012)
- (4) Procedures for Responding to Breach of PII (September 2008 and updated in March 2013)
- (5) Computer Security Incident Response Team (CSIRT) Guide (November 2011)



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

Office of Audits and Evaluations
Office of Inspector General

DATE: January 15, 2016

MEMORANDUM TO: Lawrence Gross, Jr.
Chief Information Officer


FROM: Mark F. Mulholland
Assistant Inspector General for Audits

SUBJECT: *The FDIC's Efforts to Address Recommendations Made by the
OIG Pertaining to Credentialing and Multifactor Authentication
(Assignment No. 2016-022)*

In September 2015, the FDIC Office of Inspector General (OIG) issued an audit report, entitled *The FDIC's Identity, Credential, and Access Management (ICAM) Program* (Report Number AUD-15-011, referred to herein as the ICAM audit report). The report contained two recommendations addressed to the Director, Division of Administration, to coordinate with the then Acting Chief Information Officer (CIO) and the Director, Division of Information Technology, to (1) prepare a business case that defines the goals and approach for implementing the ICAM program and (2) establish appropriate governance measures over the ICAM program. During the presentation of the ICAM audit report to the FDIC Audit Committee on November 18, 2015, the Vice Chairman expressed concern regarding the issues and risks identified during the audit and the FDIC's actions to address those issues and risks. The Vice Chairman requested that the OIG conduct additional audit work in this area during the first quarter of 2016 and report back to the Audit Committee.

The purpose of this memorandum is to advise you that we are initiating the subject audit. The objective will be to assess the FDIC's plans and actions to address the recommendations contained in the ICAM audit report. As part of the audit, we plan to periodically report to management and the Audit Committee on the FDIC's progress relative to goals and expectations and significant issues and risks that need to be addressed.

We will contact the internal control liaison within the CIO Organization to schedule an entrance conference, during which time we will discuss our plans for conducting the audit. We welcome management's views in refining our audit objective, scope, and methodology. Joseph E. Nelson will serve as the Audit Manager and Thomas F. Ritz will serve as the Team Lead.

If you have any suggestions or questions regarding this audit, please contact me at (703) 562-6316 or Joseph E. Nelson at (703) 562-6314.

cc: Martin D. Henning, EO
Rack D. Campbell, DIT
Daniel H. Bendler, DOA
James H. Angel, Jr., DOF




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

Office of Audits and Evaluations
Office of Inspector General

DATE: February 11, 2016

MEMORANDUM TO: Arthur J. Murton, Director
Office of Complex Financial Institution

Lawrence Gross, Jr.
Chief Information Officer


FROM: Mark F. Mulholland
Assistant Inspector General for Audits

SUBJECT: *Audit of the FDIC's Controls for Mitigating the Risk of an
Unauthorized Release of Sensitive Resolution Plans
(Assignment No. 2016-018)*

The purpose of this memorandum is to advise you that we have completed the planning phase of the subject audit and are proceeding with detailed field work. The audit objectives are to (a) determine the factors that contributed to a security incident involving sensitive resolution plans and (b) assess the adequacy of mitigating controls established subsequent to the incident. The sensitive resolution plans involved in the incident were submitted by financial companies pursuant to section 165(d) of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

The majority of field work will be performed at the FDIC's Virginia Square offices in Arlington, Virginia, and headquarters offices in Washington, D.C. Additional sites to be visited may be identified during the audit. We will coordinate our work with the Internal Control Liaisons (ICL) for the Office of Complex Financial Institutions, Chief Information Officer Organization, and Division of Information Technology. We will contact the ICLs in the near future to schedule an entrance conference wherein we will discuss our plans for conducting the audit field work.

If you have any questions or concerns regarding this audit prior to the entrance conference, please contact me at (703) 562-6316 or Joe Nelson, Audit Manager, at (703) 562-6314.


cc: Titus S. Simmons, OCFI
Rack D. Campbell, CIOO
Stephen M. Hanas, Legal Division
James H. Angel, Jr., DOF



Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22228

Office of Audits and Evaluations
Office of Inspector General

DATE: February 19, 2016

MEMORANDUM TO: Lawrence Gross, Jr.
Chief Information Officer


FROM: *for* Mark F. Mulholland
Assistant Inspector General for Audits

SUBJECT: *Information Security Incident Warranting Congressional Reporting*

The purpose of this memorandum is to alert you to an instance of apparent non-compliance with the Federal Information Security Modernization Act of 2014 (FISMA) and related guidance issued by the Office of Management and Budget (OMB).¹ As part of our planning work for Assignment No. 2016-023, *The FDIC's Process for Identifying and Reporting of Major Security Incidents*, we reviewed the facts and circumstances pertaining to FDIC Security Incident Number CINC-221387 (referred to herein as the incident), including whether the incident meets the criteria for being designated as "major." FISMA and OMB Memorandum M-16-03 require federal agencies, including the FDIC, to report security incidents designated as major to the Congress within 7 days of the agency having a reasonable basis to conclude that a major incident has occurred. Our analysis indicates 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, 2015.² In our view, the incident should now be reported immediately. A summary of our analysis and conclusions follows.

Agency Requirement to Report Major Security Incidents

FISMA requires federal agencies to establish procedures for detecting, reporting, and responding to security incidents. Such procedures are intended to minimize loss and destruction when security incidents occur. Among other requirements, FISMA states that agency incident response procedures must include notifying and consulting with, as appropriate, various Congressional committees for security incidents determined to be "major." According to the statute, Congressional notification is to occur not later than 7 days after the date on which there is a reasonable basis to conclude that a major security incident has occurred. FISMA also requires that the agency's annual security reports include a description of each major security incident, including the number of individuals affected if a breach of personally identifiable

¹ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 30, 2015 (referred to herein as OMB Memorandum M-16-03).

² As discussed on page 5 of this memorandum, it is possible that the incident could have been designated as major as early as November 6, 2015 (7 days after OMB issued Memorandum M-16-03) given the nature of the information involved.

information (PII) is involved. FISMA states that agencies should notify affected individuals as expeditiously as practical and without unreasonable delay.

In accordance with FISMA, OMB must define what constitutes a major security incident. Accordingly, OMB issued its Memorandum M-16-03 that describes the factors that must be considered when determining whether a security incident should be designated as major. The memorandum notes 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 should be considered major, 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.

Key Facts and Activities Related to the Incident

On October 23, 2015, the FDIC's Information Security and Privacy Staff (ISPS) supporting the Data Loss Prevention program notified the Computer Security Incident Response Team (CSIRT) of a suspected computer security incident. Specifically, ISPS informed CSIRT 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 Social Security numbers (SSNs) from customer bank data and other sensitive FDIC information, onto a single USB drive (i.e., a portable storage device). According to the Computer Security Incident Report prepared by CSIRT that same day, the sensitive information appeared to include [REDACTED] Bank Currency Transaction Reports, BSA Customer Data Reports, and a small subset of personal work and tax files. The report indicated that the employee had downloaded the information on September 16 and 17, 2015, and October 15, 2015, prior to her departure.³ It was not known at the time of the incident whether the USB drive was encrypted. The incident was also reported to the Privacy Program Office on the same day the incident was identified (i.e., October 23, 2015).

On November 3, 2015, ISPS determined that the USB drive was a personally-owned device. FDIC policy prohibits employees from storing sensitive information on non-FDIC equipment. The FDIC's Data Breach Management Team (DBMT) investigated the incident and recommended in a November 25, 2015 incident summary report that the Chief Information Office (CIO) classify the incident as a breach. In making the recommendation, the DBMT considered information contained in a detailed Incident Risk Analysis (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. The DBMT also indicated that additional work was needed to determine the impact level of the breach. On December 2, 2015, FDIC staff determined that at least 10,000 unique SSNs were involved in the breach. On the same day, the FDIC sent the former employee's attorney a letter demanding that the USB drive be returned to the FDIC not later than December 8, 2015.

³ The employee left the FDIC's employment on October 15, 2015.

On December 7, 2015, the CIO concurred with the DBMT's recommendation to classify the incident as a breach. The CIO also made a determination on behalf of the FDIC that the incident was not major.⁴ The CIO's determination was noted in a December 7, 2015 DBMT Summary Report, which stated "Based on the recommendation of the DBMT 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, does not recommend classification of the incident as a major incident." The CIO informed us that he discussed his recommendation that the incident was not major in a meeting with the Deputy to the Chairman and Chief Operating Officer/Chief of Staff, the Deputy General Counsel, and a representative of the Office of Legislative Affairs. The meeting was held on or about December 7, 2015. The CIO stated that the participants in the meeting expressed no concern with the proposed recommendation.⁵

The CIO informed us that his recommendation was based on (among other things) information that was available on the incident, the DBMT's November 25, 2015 recommendation, applicable information security guidance, and various mitigating factors, such as:

- the employee was not disgruntled when she left the FDIC;
- a belief that the employee accidentally downloaded the information when attempting to download personal information because the employee was not familiar with information technology;
- the employee was working through significant personal issues, including a divorce and not living at her residence, presenting a distraction for the employee; and
- the FDIC ultimately recovered the USB drive from the employee.

The FDIC recovered the USB drive on December 8, 2015, following extensive discussions with the employee and her attorney. As of the date of this memorandum, ISPS were continuing to investigate the incident by reviewing the downloaded information for purposes of identifying individuals whose PII was exposed through the breach. The CIO informed us that a decision had not yet been made with respect to whether the FDIC will provide notification and/or credit monitoring to the affected individuals.

⁴ The FDIC had not updated its policies and procedures to address major security incidents at the time this decision 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, this determination was not forwarded to the Chairman for review or approval.

⁵ Although not required, we noted that a written legal analysis supporting the determination had not been prepared. In addition, the CIO told us FDIC had not consulted with the OMB or US-CERT in making its determination that the incident was not major.

OIG Analysis

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, Controlled Unclassified Information (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,⁶ *or*
 - b) Any record of special importance.⁷

Based on our analysis, we determined that the incident satisfies three of the above referenced factors as demonstrated in the table below.

Factor	Definition	Characteristics of the Incident that Satisfy the Factor	Met
CUI Privacy	The confidentiality of personal information, or in some cases, PII as defined in OMB Memorandum M-07-16, <i>Safeguarding Against and Responding to the Breach of Personally Identifiable Information</i> , dated May 22, 2007, or "means of identification" as defined in 18 USC 1028 (d)(7).	On October 23, 2015, the Data Loss Prevention program identified that potentially 1,200 documents that include SSNs and bank data was copied to a USB drive by a then-departed employee. An FDIC IRA completed on or about November 25, 2015, identified that the incident included more than 1,200 documents and zip files including SSNs. In addition, the analysis noted that the files contained customer bank data with SSNs, [redacted] Bank Currency Transaction Reports, and a small subset of the data contained 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 employee's download.	✓

⁶ OMB Memorandum M-16-03 defines these thresholds to be 10,000 or more records or 10,000 or more users affected.

⁷ 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. A collection of records of special importance in the aggregate could be considered an agency High Value Asset.

Factor	Definition	Characteristics of 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 [redacted] likely to result in 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 drive that was removed from the FDIC's premises without authorization for a period of almost 2 months (i.e., October 16, 2015 through December 9, 2015). It is not possible for the FDIC to determine whether the information was compromised prior to return of the USB drive 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, 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 subject incident.

We also determined that the incident should have been reported to the Congress not later than December 9, 2015—7 days after it was determined that more than 10,000 unique SSNs were involved in the breach.⁸ At that time, the FDIC had a reasonable basis to conclude that the factors in OMB Memorandum M-16-03 were met to designate the incident as major. 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.⁹

Further, we found that the FDIC had not documented the underlying analysis of how the factors in OMB Memorandum M-16-03 were applied in determining that the incident was not major. The CIO informed us that during his meeting with the Deputy to the Chairman and Chief Operating Officer/Chief of Staff and officials in the Legal Division and Office of Legislative Affairs, the factors in the OMB memorandum were specifically considered and weighted against the aforementioned mitigating factors. In addition, according to the CIO, the incident was considered in the context of other FDIC incidents (none of which were determined by the FDIC

⁸ We independently verified that at least 10,000 unique SSNs were included in the breach. We also noted that the SSNs are often associated with other PII, such as bank account numbers, names, and addresses. In addition, the information we reviewed included Department of Treasury's Financial Crimes Enforcement Network suspect lists, copies of drivers' licenses, passports, tax returns, State of Florida reports of examination, FDIC enforcement actions, banks' wire logs, and green cards.

⁹ The information downloaded by the employee included [redacted]. Inappropriate disclosure of a [redacted] 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 [redacted] often contain PII. The FDIC's incident risk analysis completed 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.

to be major) having similar characteristics before concluding that the incident did not rise to the level of a major incident as defined in OMB Memorandum M-16-03. The CIO added that he was comfortable that the data had not been shared by the employee with other individuals and that the incident was similarly situated with other FDIC incidents in terms of the volume and nature of data involved. The CIO also told the OIG that there is no written record of the aforementioned meeting or other documented analysis that describes how the incident was analyzed for purposes of determining whether it was major.

Mitigating Factors

As discussed earlier, the CIO articulated several factors that, in his view, mitigate the potential risk or impact of the incident. Such factors include, for example, the former employee not being disgruntled at the time of her departure and the belief that the information was accidentally downloaded to the USB drive. However, OMB Memorandum 16-03 does not provide for the application of such factors in determining whether an incident is major. As part of our review, we spoke with OMB officials to ensure we had a proper understanding of the criteria in the memorandum. These officials informed us that it would be reasonable for agencies to consider factors other than those listed in the memorandum in making a determination on reporting. However, when provided hypothetical mitigating factors such as those the CIO referenced earlier, they advised us that such factors would not be an appropriate basis for determining an incident is not major and does not require reporting to the Congress. The officials added that agencies should engage in proactive communication with the Congress while incident analysis is ongoing.

Aggravating Factors

In addition to the mitigating factors that the CIO mentioned, several aggravating factors exist that may increase the risk associated with the incident. Specifically,

- The information was stored on a personal device, in an unencrypted format, and without password protection. As a result, the information was accessible to anyone with access to the device. Further, the information was outside of the FDIC's control for almost 2 months, and no technical means exists to obtain assurance that the information was not accessed by others.
- The employee's new employer is a financial services firm owned by a parent company that is based in Bangalore, India.
- The employee was not forthright with the FDIC when attempts were made to recover the information. For example, the employee repeatedly denied downloading the information and owning a portable storage device.
- In November 2015, the employee's former supervisor expressed concern about the content of the files downloaded by the employee 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.

- An employee who inappropriately copies information that he/she knows (or should know) to be highly sensitive at the end of his/her employment and who is at the same time dealing with major personal issues (e.g., a divorce, living in a hotel room, seeking employment), presents a heightened security risk profile.

Conclusion

Our analysis indicates that improvement is needed in the FDIC's process for identifying and reporting major security incidents, including the elapsed time between an initial incident and key decisions. In this case, 6 weeks elapsed between the initial reporting of the incident and a determination of whether a breach had occurred and whether it required reporting. Additional decisions regarding notification to individuals and/or organizations impacted remain outstanding—almost 4 months after the incident became known.

Our most significant and immediate concern, however, is that the FDIC needs to immediately report what we have concluded is a major incident to the appropriate Congressional committees. Doing so would be consistent with relevant statutory and policy requirements and serve to mitigate the risk of a negative financial impact on the organizations and individuals potentially affected by the breach.

As described earlier, the information involved in the incident includes a large volume of highly-sensitive PII, which increases the risk of identity theft and consumer fraud for the affected individuals. In this regard, the FDIC should also place priority attention on making a decision with respect to whether affected individuals and/or organizations will be notified, including whether such notification should be made incrementally as investigative activities continue.

We request that you provide us with a written response to this memorandum that indicates whether you will report this incident to the Congress and that describes other planned actions to address the matter, as soon as possible, but not later than Wednesday, February 24, 2016.

If you have any questions or concerns regarding this memorandum, please contact me at (703) 562-6316 or Laura A. Benton, Audit Manager, at (703) 562-6320. We appreciate your prompt attention to this matter.

cc: Rack D. Campbell, DIT
Martin D. Henning, EO
Christopher J. Farrow, CISO
James H. Angel, Jr., DOF