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.

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.

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.

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.

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

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

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

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.