Office of Inspector General

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

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

July 2016

Office of Inspector General

Executive Summary

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

Report No. AUD-16-003
July 2016

Why We Did The Audit

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

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

Background

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

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

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

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

Audit Results

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

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

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

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

Recommendations and Corporation Comments

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

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

Contents

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

Office of Audits and Evaluations
Office of Inspector General

DATE: July 6, 2016

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

Lawrence Gross, Jr.
Chief Information Officer

Arthur J. Murton, Director
Office of Complex Financial Institutions

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

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

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

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

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

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

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

Background

The FDIC's Information Security Program

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

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

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

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

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

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

The Sensitive Nature of Resolution Plans

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

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

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

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

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

The Security Incident Involving Resolution Plans

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

[3] Based on the activity detected by the DLP tool, the employee copied the Executive Summary and the narrative description of the SIFI's resolution strategy for each of the three plans, but did not copy the supporting appendices or documents containing other information required by the Final Rule.

[4] OCFI's policy memorandum, entitled *OCFI Title 1 Security Practices for Review of Resolution Plans Submitted to OCFI under the §165(d) Rule or under the IDI Rule*.

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

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

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

Audit Results

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

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

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

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

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

Factors that Contributed to the Incident

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

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

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

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

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

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

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

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

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

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

Risks Posed by the Employee and the FDIC's Response

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

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

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

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

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

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

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

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

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

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

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

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

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

Efforts to Establish an Insider Threat Program at the FDIC

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

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

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

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

Recommendation

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

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

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

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

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

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

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

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

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

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

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

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

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

Recommendations

We recommend that the CIO:

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

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

We recommend that the Director, OCFI:

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

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

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

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

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

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

Recommendation

We recommend that the Director, OCFI:

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

OCFI Was Not Able to Monitor All Downloading of Resolution Plans

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

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

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

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

- limiting the ability of employees to view, download, and print resolution plans stored in ODM to a subset of SIFIs based on the specific job duties of the employee;

- increasing the frequency of reviews of employee access to resolution plans in ODM from bi-monthly to monthly to ensure access privileges remain consistent with business needs;

- coordinating with ISPS to expand the parameters used to block email communications addressed to non-FDIC email accounts that appear to contain content related to resolution plans;

- conducting weekly reviews of print activity by ODM users with access to sensitive resolution plans to identify and investigate suspicious activity (e.g., large print jobs); and

[11] As noted in the following section of this report, OCFI has begun to monitor print activity for ODM users with access to resolution plans.

- conducting bi-weekly comparisons of recently separated or transferred employees to ODM users with access to resolution plans to help ensure that access is promptly disabled, when appropriate.

OCFI had not yet developed written policies, procedures, and assessment plans to govern the controls described above. Accordingly, we did not have criteria against which to test the effectiveness of these controls. However, we did review documentation confirming that OCFI had begun implementing each of these controls. OCFI officials indicated that they intend to develop policies, procedures, and assessment plans in the near future to ensure that the new and enhanced controls are repeatable, consistent, and disciplined; operating as intended; and producing the desired outcomes with respect to meeting OCFI's security requirements. Doing so would be consistent with GAO standards, FDIC policy, and NIST guidance.

Recommendation

We recommend that the Director, OCFI:

6. Develop appropriate policies and procedures that address the new and enhanced security controls established by OCFI subsequent to the incident and establish and implement plans to periodically assess the effectiveness of those controls.

Corporation Comments and OIG Evaluation

The Deputy to the Chairman, Chief Operating Officer, and Chief of Staff; the CIO; and the Director, OCFI; provided a joint written response, dated June 28, 2016, to a draft of this report. The response is provided in its entirety in Appendix 4. In the response, FDIC management concurred with all six of the report's recommendations. A summary of the Corporation's corrective actions is presented in Appendix 5. The planned actions are responsive to the recommendations and the recommendations are resolved.

Objectives, Scope, and Methodology

Objectives

The objectives of the audit were to (a) determine the factors that contributed to the security incident involving sensitive resolution plans and (b) assess the adequacy of mitigating controls established subsequent to the incident.

We performed audit fieldwork from February through May 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope and Methodology

To determine the factors that contributed to the incident, we first interviewed officials in OCFI, DOA, RMS, ISPS, DIT, and the Legal Division to obtain an understanding of the facts and circumstances surrounding the incident and the security controls that should have been implemented for the employee at that time. Next, based on the results of these interviews and our review of relevant policies, procedures, guidelines, and records, we identified the following seven controls established by FDIC management at the time of the incident that we determined to be particularly relevant.

1. The employee should have received a favorable determination from DOA on a high-risk background investigation within the last 5 year(s), or been the subject of an ongoing, initial high-risk background investigation.

2. The employee should have completed an OCFI *Acknowledgement of Confidentiality Obligations* within 2 years of departure.

3. The employee should have affirmed the responsibilities agreement at the end of the FDIC's online Information Security and Privacy Awareness Training within 1 year of departure.

4. The employee should have been technically restricted from copying electronic information, including sensitive resolution plans, from the FDIC network to removable media.

5. The employee should have been subject to the FDIC's performance management program.

6. The employee should have been subjected to possible disciplinary action for violating an FDIC information security policy in April 2015.

7. The employee should have certified when completing the Corporation's pre-exit clearance procedures that no sensitive information related to financial institutions would be taken from the FDIC upon departure.[12]

We then assessed whether each of these controls was implemented for the employee by examining records related to the incident and evidence of control implementation, such as personnel files and training records. In addition to the failure of control number 4 listed above for the employee, we identified control gaps (i.e., unestablished controls) that, taken together, we considered to be the principal factors that contributed to the incident.

To assess the adequacy of mitigating controls established subsequent to the incident, we interviewed OCFI and DIT officials to learn about new or enhanced security controls and considered the extent to which these controls addressed the factors that contributed to the incident. We also reviewed documentation to determine whether implementation of each of these controls had begun. However, because OCFI had not yet developed written policies, procedures, and assessment plans to govern these controls, we did not have criteria against which to test the effectiveness of the controls. Accordingly, we did not perform such tests.

The primary criteria used in the audit was as follows:

- Section 112(d)(5) of the Dodd-Frank Act (12 U.S.C. § 5322), which states that members of the Financial Stability Oversight Council, including the FDIC, ''shall maintain the confidentiality of any data, information, and reports submitted under'' title I of the statute (which includes section 165(d)).

- The Final Rule, entitled *Resolution Plans Required*, which states that institutions that file resolution plans are to indicate to the regulators which portions of the plans are confidential and which portions can be made public.

- FISMA, which requires federal agencies, including the FDIC, to (a) develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency and (b) provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, or disclosure of information collected or maintained by the agency.

- Security guidelines issued by NIST that assist agencies in defining security requirements for their information systems.

[12] Completion of the pre-exit clearance procedures is designed to help safeguard FDIC-owned property and interests when employees leave the Corporation. We did not audit the completion of the pre-exit clearance procedures in their totality.

Objectives, Scope, and Methodology

- GAO's *Standards for Internal Control in the Federal Government*, dated September 2014, that defines an overall framework for establishing and maintaining effective internal controls in federal agencies.

- Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, which requires agencies that handle classified information to establish insider threat programs.

- *Presidential Memorandum—National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, which provides direction and guidance to federal departments and agencies in developing effective insider threat programs. The memorandum requires departments and agencies with access to classified information, or that operate or access classified computer networks, to implement an insider threat program.

- FDIC information security policies, procedures, and guidelines designed to protect sensitive information from unauthorized disclosure. A key policy with respect to safeguarding resolution plans is OCFI's memorandum, entitled *OCFI Title 1 Security Practices for Review of Resolution Plans Submitted to OCFI under the §165(d) Rule or under the IDI Rule*, dated June 2013.

In planning this audit, we considered the results, conclusions, and recommendations pertaining to our audit report, entitled *The FDIC's Controls for Safeguarding Sensitive Information in Resolution Plans Submitted Under the Dodd-Frank Act* (Report No. AUD-14-008, dated July 3, 2014).

We performed our audit work at the FDIC's offices in Arlington, Virginia, and Washington, D.C.

Glossary of Terms

Term	Definition
Confidential Information	Within the context of the Dodd-Frank Act, the terms confidential and confidentiality have been defined by the Final Rule to mean not releasing information from the resolution plans that the submitter considers confidential and not releasable to the public under the Freedom of Information Act (5 U.S.C. § 552) or FRB and/or FDIC regulations (12 Code of Federal Regulations (C.F.R.) parts 261 and 309). Under FISMA (Public Law (P.L.) No. 113-283), the terms confidential and confidentiality are defined as preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information.
Conflict of Interest Statement	In the context of this report, a Conflict of Interest Statement is completed by an FDIC employee to identify any conflicts of interest with respect to SIFIs prior to obtaining access to sensitive resolution plans so that only appropriate access will be granted.
Counterintelligence	Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.
Data Loss Prevention	Sometimes referred to as data leak prevention or information loss prevention, the term refers to a strategy for mitigating the risk of end users transmitting sensitive information outside of the organization. In the context of this report, the term refers to a software tool designed to detect and, if enabled, prevent potential data breaches by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
Major Incident	An information security incident that meets the criteria defined in the Office of Management and Budget's Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*. FISMA requires federal agencies to notify and consult with, as appropriate, the Congressional Committees referenced in the statute for major incidents. According to FISMA, Congressional notification and consulting is to occur not later than 7 days after the date on which there is a reasonable basis to conclude that a major incident has occurred.
Microsoft Windows Active Directory®	An IT service in the Windows Server® operating system platform that is used to centrally manage user accounts and security settings (including access).
Phishing	A digital form of social engineering that uses authentic looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information.

Glossary of Terms

Term	Definition
Resolution Plans	Section 165(d) of the Dodd-Frank Act requires each bank holding company with total consolidated assets of $50 billion or more and each nonbank financial company designated by the Financial Stability Oversight Council (FSOC) for enhanced supervision by the FRB to report periodically to the FDIC, FRB, and FSOC on the plan of such company for its rapid and orderly resolution in the event of material financial distress or failure. To implement this requirement, the FDIC and FRB jointly issued a Final Rule, entitled *Resolution Plans Required*, on November 1, 2011, that requires financial companies covered by the statute to submit resolution plans describing the company's strategy for a rapid and orderly resolution under the Bankruptcy Code in the event of material financial distress or failure of the company.
Social Engineering	In the context of information security, social engineering refers to the psychological manipulation of people causing them to perform actions or divulging confidential information.
Sensitive Information	In general, sensitive information is information that contains an element of confidentiality. It includes information that is exempt from disclosure by the Freedom of Information Act and information whose disclosure is governed by the Privacy Act of 1974 (5 U.S.C. § 552a). Sensitive information requires a high level of protection from loss, misuse, and unauthorized access or modification.
Systemically Important Financial Institution	Refers to bank holding companies with $50 billion or more in total consolidated assets and nonbank financial companies designated by the FSOC for FRB supervision and enhanced prudential standards of the Dodd-Frank Act (12 U.S.C. §§ 5322 and 5323).

Abbreviations and Acronyms

Abbreviation/Acronym	Explanation
AD	Microsoft Windows Active Directory®
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DIT	Division of Information Technology
DLP	Data Loss Prevention
DOA	Division of Administration
EMC	Executive Management Committee
FISMA	Federal Information Security Modernization Act of 2014
FRB	Board of Governors of the Federal Reserve System
FSOC	Financial Stability Oversight Council
GAO	Government Accountability Office
IPP	Internal Protection Program
ISM	Information Security Manager
ISPS	Information Security and Privacy Staff
NIST	National Institute of Standards and Technology
OCFI	Office of Complex Financial Institutions
ODM	OCFI Documentum
OIG	Office of Inspector General
PIP	Performance Improvement Plan
RMS	Division of Risk Management Supervision
SEPS	Security and Emergency Preparedness Section
SIFI	Systemically Important Financial Institution
SP	Special Publication
USB	Universal Serial Bus
U.S.C.	United States Code

Corporation Comments

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C., 20429

DATE: June 28, 2016

MEMORANDUM TO: Mark F. Mulholland
Assistant Inspector General for Audits

FROM: Barbara A. Ryan /Signed/
Deputy to the Chairman and Chief Operating Officer/Chief of Staff

Arthur J. Murton, Director /Signed/
Office of Complex Financial Institutions

Lawrence Gross /Signed/
Chief Information Officer

SUBJECT: Management Response to the Draft OIG Audit Report Entitled *The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans* (Assignment No. 2016-018)

The Federal Deposit Insurance Corporation (FDIC) has completed its review of the Office of Inspector General's (OIG) draft audit report entitled *The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans Submitted Under the Dodd-Frank Act* (Assignment No. 2016-018), dated June 8, 2016.

We appreciate the OIG's analysis and findings regarding the FDIC's controls for safeguarding resolution plans. We recognize the need to improve those controls and address identified weaknesses. The draft report notes that the FDIC has recently implemented a number of controls designed to mitigate the information security risks associated with sensitive resolution plans. It also acknowledges that the FDIC has a number of long-standing controls designed to mitigate risks associated with trusted insiders. However, the report identifies six recommendations for improvements to strengthen information security and FDIC management concurs with these recommendations. We are committed to addressing each of the recommendations to further strengthen our controls and lower the risk of harm from the unauthorized release of sensitive information.

Our detailed response below is organized by recommendation and contains actions planned or in process and those that have been completed.

Recommendation 1: The OIG recommends that the Deputy to the Chairman and Chief Operating Officer/Chief of Staff (COO/COS) coordinate with the Executive Management Committee (EMC) to establish a corporate-wide insider threat program that is consistent with NIST-recommended practices and applicable laws, Executive Orders, national strategies, directives, regulations, policies, standards, and guidelines.

Corporation Comments

Management Decision: Concur

Corrective Actions: As noted by the OIG, with respect to insider threats, the FDIC has a number of long-standing controls designed to mitigate risks associated with trusted insiders, including background investigations, periodic inspections of FDIC facilities to identify security concerns, employee non-disclosure agreements, a Data Loss Prevention (DLP) tool, and programs to help employees with personal issues.

In 2014 and 2015, the FDIC began to take steps toward establishing a formal insider threat program by developing draft governance, policy, and procedures documents, and by initiating interdivisional discussions on the topic. However, as of October 2015, the insider threat program had not been implemented. As noted by the OIG, such a program would have better enabled the FDIC to deter, detect, and mitigate the risks posed by the employee.

The COO/COS, with the EMC, has engaged a cross-disciplinary team composed of FDIC executive-level staff from the human resources, legal, physical security, and information system areas to formally establish a corporate-wide insider threat program consistent with NIST-recommended practices and applicable laws, Executive Orders, national strategies, directives, regulations, policies, standards, and guidelines. This team is finalizing the FDIC's insider threat program policy statement and governance structure. The FDIC is committed to completing this by October 28, 2016.

A key component of the formal insider threat program is the establishment of an insider threat working group composed of key stakeholder groups (including representatives from the Division of Administration/Security, CIO/CISO, Legal Division and other major divisions/offices) and chaired by a senior FDIC official designated as being responsible for implementing and providing oversight of the program. The insider threat working group will focus on identifying, mitigating, and preventing malicious insider threat activity. It will meet on a regular basis and convene ad hoc meetings to address exigent threats or concerns to the FDIC as needed. The FDIC is committed to establishing the insider threat working group by October 28, 2016.

Employee awareness will be critical to the success of the FDIC's insider threat program. Introductory outreach briefings on the program will be conducted in both headquarters and regional offices to ensure employee awareness of the new program and its requirements. The FDIC is committed to conducting information awareness briefings from the date of program implementation through the end of the year and to integrating insider threat program employee awareness training into the existing security training module by December 30, 2016.

Completion Dates: From October 2016 through December 2016 as identified above.

Corporation Comments

Recommendation 2: The OIG recommends that the CIO immediately test the effectiveness of the control designed to prohibit network users from copying information to removable media to confirm that the control operates as intended.

Management Decision: Concur

Corrective Action: The OIG noted that a key security control designed to prevent employees with access to sensitive resolution plans from copying electronic information to removable media failed to operate as intended. Between October 2015 and April 2016, the Division of Information Technology (DIT) coordinated tests with OCFI and others to ensure the software that prohibits copying files to removable media was working properly. While the majority of the tests were successful, some tests identified defects in limited situations. We are now installing a new software version that addresses the observed defects and plan that installation to be complete by August 26, 2016. Documentation of the test steps and the results of the test will be improved. In addition, DIT will develop a comprehensive test plan and use it to re-evaluate regularly the effectiveness of the software that prohibits users from copying information to removable media.

Completion Date: August 26, 2016

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

Management Decision: Concur

Corrective Action: The CIO organization will coordinate with division and office directors to identify and update relevant directives and procedures to ensure that they are consistent with the decision to discontinue copying information to removable media. Updated directives and procedures will include protocols for managing any limited exceptions and requirements for regular testing of the control's effectiveness.

Completion Date: September 30, 2016

Recommendation 4: The OIG recommends that the Director, OCFI, assign a dedicated information security manager to support OCFI.

Management Decision: Concur

Corporation Comments

Corrective Action: OCFI will work with DOA's Human Resources Branch to announce and fill a vacancy for a dedicated information security manager (ISM) position, rather than continuing to share an ISM with the Division of Insurance and Research. A dedicated ISM will ensure that appropriate security controls are in place to better protect OCFI's resolution plan information and information systems.

Completion Date: December 30, 2016

Recommendation 5: The OIG recommends that the Director, OCFI, evaluate whether employees should continue to be allowed to store copies of sensitive resolution plans outside of OCFI Documentum (ODM), and if so, determine what additional mitigation strategies may be warranted to address the associated risk.

Management Decision: Concur

Corrective Action: OCFI is updating its policy regarding the storage of sensitive information. The revised policy will specifically prohibit the practice of storing sensitive resolution plans outside of ODM, including in other secure locations such as hard drives and personal U: drives. It will also address print and download controls. We will continually monitor this policy as the FDIC considers new technologies to store and secure sensitive information.

Completion Date: September 30, 2016

Recommendation 6: The OIG recommends that the Director, OCFI, develop appropriate policies and procedures that address the new and enhanced security controls established by OCFI subsequent to the incident and establish and implement plans to periodically assess the effectiveness of those controls.

Management Decision: Concur

Corrective Action: OCFI is revising its policies and procedures to address the new and enhanced security controls established subsequent to the incident, as described in the OIG's draft report. OCFI will also develop comprehensive procedures that will incorporate control activities to mitigate program risks and ensure that resolution plans are adequately safeguarded. In addition to developing comprehensive policies and procedures, OCFI will conduct internal reviews to periodically test these controls to ensure that the controls are repeatable, consistent, disciplined, and operating as intended.

Completion Date: September 30, 2016

Questions regarding this response should be directed to Rack Campbell at (703) 562-1422.

Corporation Comments

cc: James H. Angel, Jr., Deputy Director, DOF, Corporate Management Control
Stephen M. Hanas, Legal Division
Titus S. Simmons, Lead Planning and Resource Management Analyst, OCFI, Organizational, Planning & Resource Management
Roderick E. Toms, Acting CISO, Information Security & Privacy
Russell G. Pittman, Director, DIT
Isaac E. Hernandez, Deputy Director, DIT, Infrastructure Services Branch
Steven P. Anderson, Deputy Director, DIT, Business Administration Branch
Rack D. Campbell, Supervisory IT Specialist, DIT, Audit and Internal Control

.

Summary of the Corporation's Corrective Actions

This table presents corrective actions taken or planned by the Corporation in response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The FDIC will finalize the insider threat program policy statement and governance structure, establish an insider threat working group to implement and oversee the program, and provide awareness briefings to employees on the new program and its requirements.	12/30/2016	$0	Yes	Open
2	DIT will complete the installation of new software that addresses known vulnerabilities in the security control designed to prevent employees from copying sensitive information to removable media. In addition, the CIO Organization will develop a test plan and use it to re-evaluate regularly the effectiveness of the control.	8/26/2016	$0	Yes	Open
3	The FDIC will identify and update relevant directives and procedures to ensure they are consistent with the management decision to discontinue copying information to removable media. Updated directives and procedures will include protocols for managing exceptions and requirements for regular control testing.	9/30/2016	$0	Yes	Open
4	The FDIC will announce and fill a position for a dedicated ISM to support OCFI.	12/30/2016	$0	Yes	Open
5	OCFI will update its policy regarding the storage of sensitive information to prohibit the practice of storing sensitive resolution plans outside of ODM. The update will also address controls over printing and downloading.	9/30/2016	$0	Yes	Open
6	OCFI will revise its policies and procedures to address new and enhanced security controls	9/30/2016	$0	Yes	Open

Summary of the Corporation's Corrective Actions

	established subsequent to the incident involving sensitive resolution plans and described in this report. In addition, OCFI will develop comprehensive procedures that incorporate control activities to mitigate program risks and ensure that resolution plans are adequately safeguarded. Further, OCFI will conduct internal reviews to periodically test these controls.				

[a] Resolved – (1) Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but alternative action meets the intent of the recommendation.
(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Recommendations will be closed when (a) Corporate Management Control notifies the OIG that corrective actions are complete or (b) in the case of recommendations that the OIG determines to be particularly significant, when the OIG confirms that corrective actions have been completed and are responsive.