United States Government Accountability Office

Report to the Chairman, Federal Deposit Insurance Corporation

May 2017

INFORMATION SECURITY

FDIC Needs to Improve Controls over Financial Systems and Information

Accessible Version

GAO-17-436

May 2017

INFORMATION SECURITY

FDIC Needs to Improve Controls over Financial Systems and Information

GAO Highlights

Highlights of GAO-17-436, a report to the Chairman, Federal Deposit Insurance Corporation

Why GAO Did This Study

FDIC has a demanding responsibility enforcing banking laws, regulating financial institutions, and protecting depositors. Because of FDIC's reliance on information systems, effective information security controls are essential to ensure that the corporation's systems and information are adequately protected from inadvertent or deliberate misuse, improper modification, unauthorized disclosure, or destruction.

As part of its audit of the 2016 and 2015 financial statements of the Deposit Insurance Fund and the Federal Savings and Loan Insurance Corporation Resolution Fund, which are administered by FDIC, GAO assessed the effectiveness of the corporation's controls in protecting the confidentiality, integrity, and availability of its financial systems and information. To do so, GAO examined security policies, procedures, reports, and other documents; tested controls over key financial applications; and interviewed FDIC personnel.

What GAO Recommends

GAO is recommending that FDIC take one action to more fully implement its information security program. In a separate report with limited distribution, GAO made six recommendations to FDIC to address newly identified weaknesses in access and configuration management controls. In commenting on a draft of this report, FDIC agreed with GAO's recommendation and stated that corrective actions to implement the recommendation will be completed by July 2017.

View GAO-17-436. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

The Federal Deposit Insurance Corporation (FDIC) implemented numerous information security controls intended to protect its key financial systems. However, further actions are needed to address weaknesses in access controls—including boundary protection, identification and authentication, and authorization controls—and in configuration management controls. For example, the corporation did not sufficiently isolate financial systems from other parts of its network, ensure that users would be held accountable for the use of a key privileged account, or establish a single, accurate listing of all IT assets in its environment.

The corporation established a comprehensive framework for its information security program and implemented many aspects of its program. For example, FDIC (1) defined security categories for the general support systems we reviewed based on risk; (2) assessed the risk from control deficiencies identified during security control tests; and (3) conducted a disaster recovery test of its general support systems and mission-critical applications. In addition, FDIC addressed 15 of the 21 previously reported weaknesses that were unresolved as of December 31, 2015, as indicated in the following table.

Status of GAO Information Security Recommendations to FDIC as of December 2016

Information security control area	Not implemented at the beginning of 2016	Implemented during 2016	Actions still in progress
Access controls	15	13	2
Other controls	4	1	3
Information security program	2	1	1
Total	**21**	**15**	**6**

Source: GAO analysis of FDIC information. | GAO-17-436

However, an underlying reason for many of the information security weaknesses identified during GAO's review was that FDIC did not fully implement other aspects of its program. For example, the corporation did not (1) include necessary information in procedures for granting access to a key financial application and (2) fully address the FDIC Office of the Inspector General's finding that the corporation did not always identify and report major security incidents in a timely manner.

Until FDIC takes the necessary steps to address both new and previously reported control deficiencies, its sensitive financial information and resources will remain at increased risk of inadvertent or deliberate misuse, improper modification, unauthorized disclosure, or destruction. The combination of the continuing and new information security control deficiencies in access and configuration management controls, considered collectively, represent a significant deficiency in FDIC's internal control over financial reporting as of December 31, 2016.

Contents

Letter 1

Background 2
FDIC Continues to Implement Controls, but Collective Weaknesses Require Management Attention 6
Conclusions 22
Recommendations for Executive Action 23
Agency Comments and Our Evaluation 23

Appendix I: Objective, Scope, and Methodology 26

Appendix II: Comments from the Federal Deposit Insurance Corporation 29

Appendix III: GAO Contacts and Staff Acknowledgments 31

Appendix IV: Accessible Data 32

Agency Comment Letter 32

Abbreviations

CIO	Chief Information Officer
FDIC	Federal Deposit Insurance Corporation
FIPS Pub.	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act of 2014
ID	identification
IT	information technology
ISM	Information Security Manager
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SP	Special Publication

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 31, 2017

The Honorable Martin J. Gruenberg
Chairman
Federal Deposit Insurance Corporation

Dear Chairman Gruenberg:

The Federal Deposit Insurance Corporation (FDIC) has a demanding responsibility to enforce banking laws, regulate banking institutions, and protect depositors. In carrying out its financial and mission-related operations, the corporation relies extensively on computerized systems. Because the corporation plays an important role in maintaining public confidence in financial institutions, issues that affect the confidentiality, integrity, and availability of the sensitive information maintained on its systems are of paramount concern. In particular, effective information security controls are essential to ensure that the corporation's systems and information are being adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

As part of our audit of FDIC's calendar year 2016 and 2015 financial statements of the Deposit Insurance Fund and the Federal Savings and Loan Insurance Corporation Resolution Fund, we assessed the effectiveness of the corporation's information security controls over key financial systems, data, and networks. As highlighted in our related report on the audit of these financial statements,[1] during 2016, FDIC made progress addressing previously reported control deficiencies related to its information systems. Key corrective actions included improving controls for authorizing users' access to financial applications and for logging and monitoring financial applications to detect potentially malicious activity.

However, the collective effect of the deficiencies in information security from prior years that continued to exist in calendar year 2016, along with new deficiencies in access and configuration management controls that we identified during our calendar year 2016 and 2015 audit (discussed in this report), are serious enough to merit the attention of those charged with governance of FDIC. Therefore, they represented a significant deficiency in FDIC's internal control over financial reporting systems as of

[1]GAO, *Financial Audit: Federal Deposit Insurance Corporation Funds' 2016 and 2015 Financial Statements*, GAO-17-299R (Washington, D.C.: February 15, 2017).

December 31, 2016,[2] based on criteria established under the *Federal Managers' Financial Integrity Act of 1982*.[3]

Our objective for this audit was to determine the effectiveness of the corporation's information security controls in protecting the confidentiality, integrity, and availability of its financial systems and information. This work was performed to support our opinion on FDIC's internal control over financial reporting as of December 31, 2016. See appendix I for more details on our objective, scope, and methodology.

We conducted this audit 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

FDIC was established by Congress to maintain the stability of and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions, and resolving troubled institutions. Congress created FDIC in 1933[4] in response to the

[2]A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit the attention of those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

[3]31 U.S.C. § 3512(c) and (d).

[4]*Federal Deposit Insurance Corporation Act*, June 16, 1933, Ch. 89, § 8.

thousands of bank failures that had occurred throughout the late 1920s and early 1930s.[5]

The Bank Insurance Fund and the Savings Association Insurance Fund were established as FDIC responsibilities under the *Financial Institutions Reform, Recovery, and Enforcement Act of 1989*, which sought to reform, recapitalize, and consolidate the federal deposit insurance system.[6] The Bank Insurance Fund and the Savings Association Insurance Fund merged into the Deposit Insurance Fund on February 8, 2006, as a result of the passage of the *Federal Deposit Insurance Reform Act of 2005*.[7] As administrator of the Deposit Insurance Fund, FDIC insures the deposits of banks and savings associations (insured depository institutions). In cooperation with other federal and state agencies, the FDIC promotes the safety and soundness of insured depository institutions by identifying, monitoring, and addressing risks to the Deposit Insurance Fund.

FDIC is also the administrator of the Federal Savings and Loan Insurance Corporation Resolution Fund. This fund was created to close out the business of the former Federal Savings and Loan Insurance Corporation and liquidate the assets and liabilities transferred from the former Resolution Trust Corporation.[8]

FDIC Relies on Computer Systems to Support Its Mission and Financial Reporting

FDIC relies extensively on computerized systems to support its mission, including financial operations, and to store the sensitive information that it collects. The corporation uses local and wide area networks to interconnect its systems.

[5]FDIC is an independent agency of the federal government and receives no direct federal appropriations; it is funded by premiums that banks and thrift institutions pay for deposit insurance coverage and from earnings on investments in U.S. Treasury securities. Additionally, FDIC realizes some income from failed financial institutions for services it performs on their behalf.

[6]Pub. L. No. 101-73, § 211, 103 Stat. 183, 218-22 (Aug. 9, 1989).

[7]Pub. L. No. 109-171, Title II, Subtitle B, § 2102 (Feb. 8, 2006).

[8]A third fund to be managed by FDIC, the Orderly Liquidation Fund, established by the *Dodd-Frank Wall Street Reform and Consumer Protection Act*, Pub. L. No. 111-203, § 210(n),124 Stat. 1376, 1506 (July 21, 2010), is unfunded and conducted no transactions during the fiscal years covered by this audit.

To support its financial management functions, FDIC uses, among other things, the following information technology (IT) resources:

- a corporate-wide system that functions as a unified set of financial and payroll systems that are managed and operated in an integrated fashion;
- a system to calculate and collect FDIC deposit insurance premiums and Financing Corporation[9] interest amounts from insured institutions;
- a Web-based application that provides full functionality to support franchise marketing,[10] asset marketing, and asset management;
- an application and Web portal to provide acquiring institutions with a secure method for submitting required data files to FDIC;
- computer programs used to derive the corporation's estimate of losses from shared loss agreements;[11]
- a system to request access to and receive permission for the computer applications and resources available to its employees, contractors, and other authorized personnel; and
- a primary receivership and subsidiary financial processing and reporting system.

Cyber Threats Facing Federal Systems Continue to Evolve

The federal government has seen a marked increase in the number of information security incidents affecting the integrity, confidentiality, and availability of government information, systems, and services. Without proper safeguards, computer systems are vulnerable to individuals and

[9]The Financing Corporation, established by the *Competitive Equality Banking Act of 1987*, is a mixed-ownership government corporation with its primary purpose being to function as a financing vehicle for the Federal Savings and Loan Insurance Corporation. Effective December 12, 1991, as provided by the *Resolution Trust Corporation Refinancing, Restructuring and Improvement Act of 1991*, the Financing Corporation's ability to issue new debt was terminated. Outstanding Financing Corporation bonds, which are 30-year noncallable bonds with a principal amount of approximately $8.1 billion, mature in 2017 through 2019.

[10]Franchise marketing is a process where the FDIC markets troubled institutions to healthy insured depository institutions to help maintain financial system stability and public confidence.

[11]Under a shared loss agreement, FDIC absorbs a portion of the loss on specified assets of a failed bank that are purchased by an acquiring bank.

groups with malicious intentions who can intrude and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks. Cyber-based threats to information systems and cyber-related critical infrastructure can come from sources internal and external to the organization. External threats include the ever-growing number of cyber-based attacks that can come from a variety of sources such as individuals, groups, and countries who wish to do harm to an organization's systems. Internal threats include errors or mistakes, as well as fraudulent or malevolent acts by employees or contractors working within an organization.

Federal Law and Guidance Provide a Framework for Protecting FDIC's Federal Information and Systems

Under the *Federal Information Security Modernization Act of 2014* (FISMA),[12] the Chairman of FDIC is responsible for, among other things, (1) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the agency's information systems and information; (2) ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control; and (3) delegating to the corporation's Chief Information Officer (CIO) the authority to ensure compliance with the requirements imposed on the agency under FISMA.

FISMA states that the CIO is responsible for developing and maintaining a corporate-wide information security program and for developing and maintaining information security policies, procedures, and control techniques that address all applicable requirements. FISMA also states that the CIO is to designate a senior agency information security officer to carry out the CIO's responsibilities for information security under the law. In most federal organizations, this official is referred to as the Chief Information Security Officer.

[12]The *Federal Information Security Modernization Act of 2014* (FISMA), Pub. L. No. 113-283 (Dec. 18, 2014), partially superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in the 2014 law. FISMA 2002 requirements relevant here that were incorporated and continued in the 2014 law, and to other relevant FISMA 2002 requirements that were unchanged by the 2014 law and continue in full force and effect.

At FDIC, the CIO is responsible for, among other things, (1) establishing the information security risk management program and ensuring that it is properly implemented; (2) establishing the overall strategy for how the corporation frames, assesses, responds to, and monitors information security risks; and (3) establishing and promulgating agency-wide information security risk awareness programs and practices. The responsibilities of the FDIC Chief Information Security Officer include, among other things, (1) overseeing the corporation's information technology security risk management program; (2) providing information security standards, control frameworks, security policy, best practices, and security architecture oversight; (3) ensuring appropriate staffing and support of all information security positions that support the risk management program; and (4) managing and maintaining the continuous monitoring program.

FDIC Continues to Implement Controls, but Collective Weaknesses Require Management Attention

For calendar years 2016 and 2015, FDIC implemented numerous information security controls intended to protect its key financial systems. In addition, the corporation addressed 15 of 21 recommendations to mitigate control weaknesses that we had previously identified in our reports in 2013, 2014, 2015, and 2016. Nevertheless, weaknesses remained in FDIC's implementation of access, configuration management, and information security program controls that threaten the confidentiality, integrity, and availability of its financial systems and information.

As we have previously reported,[13] the collective effect of weaknesses in access and configuration management controls, both new and unresolved from previous audits, contributed to our determination that FDIC had a significant deficiency in internal control over financial reporting as of December 31, 2016.

[13]GAO-17-299R.

Access Control Weaknesses Increased the Risk of Inappropriate Data Access

An agency can better protect the resources that support its critical operations and assets from unauthorized access, disclosure, modification, or loss by designing and implementing controls for protecting information system boundaries, identifying and authenticating users, restricting user access to only what has been authorized, encrypting sensitive data, and auditing and monitoring systems to detect potentially malicious activity, among other actions. Although FDIC had implemented numerous controls in these areas, weaknesses nevertheless continued to challenge the corporation in ensuring the confidentiality, integrity, and availability of its information and information systems.

Financial Systems Were Not Sufficiently Isolated

Boundary protection controls are intended to restrict logical access into and out of networks and control connectivity to and from network-connected devices. Any connections to the Internet or to other external and internal networks or information systems should occur through controlled interfaces (for example, gateways, routers, switches, and firewalls). In addition, networks should be appropriately configured to adequately protect access paths between systems; this can be accomplished through the use of access control lists and firewalls.

National Institute of Standards and Technology (NIST) guidance[14] recommends that organizations employ boundary protection mechanisms to separate organization-defined information system components supporting organization-defined missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Consistent with NIST guidance, Office of Management and Budget Circular A-130 requires agencies to isolate sensitive or critical information resources (e.g., information systems, system components, applications, databases, and information) into separate security domains with appropriate levels of protection based on the sensitivity or criticality of those resources.

[14]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication (SP) 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

FDIC did not implement sufficient internal boundary protection controls on its network to isolate financial systems from other parts of its network. Although the corporation partially isolated financial systems from other parts of the environment using virtual local area networks, it did not always implement controls on network devices to prevent unauthorized users and systems from communicating with the financial systems.

According to FDIC, a plan to isolate sensitive systems had been made, but implementation of the plan had been delayed due to other competing priorities. Until it appropriately isolates its financial systems, FDIC faces increased risk that unauthorized or malicious attempts to communicate with its financial systems could go undetected.

FDIC Did Not Adequately Ensure Accountability for the Use of A Key Privileged Account

Identification is the process of distinguishing one user from all others, usually through user identifications (ID). These are important because they are the means by which specific access privileges are assigned and recognized by the computer. However, because the confidentiality of a user ID is typically not protected, other means of authenticating users—that is, determining whether individuals are who they say they are—are typically implemented. The combination of identification and authentication—such as user account-password combinations—provides the basis for establishing accountability and for controlling access to the system. NIST SP 800-53, revision 4 recommends that agency information systems uniquely identify and authenticate organizational users or processes acting on behalf of organizational users.

FDIC did not implement sufficient controls to ensure that users would be held accountable for the use of a key privileged account. Although the corporation employed a software tool to control access to privileged accounts, it did not use the tool to control access to a privileged account that was used by multiple engineers to manage the corporation's virtual environment. As a result, FDIC's ability to attribute authorized, as well as unauthorized, system activity to specific individuals could be diminished.

Authorization Controls Were Improved, but More Consistent Implementation is Needed

Authorization is the process of granting or denying access rights and privileges to a protected resource, such as a network, system, application, function, or file. A key component of granting or denying

access rights is the concept of "least privilege," which refers to granting a user only the access rights and permissions needed to perform official duties.

To restrict a legitimate user's access to only those programs and files needed, organizations establish user access rights: allowable actions that can be assigned to a user or to groups of users. File and directory permissions are rules that are associated with a particular file or directory, regulating which users can access it—and the extent of their access rights. To avoid unintentionally giving a user unnecessary access to sensitive files and directories, an organization should give careful consideration to its assignment of rights and permissions.

NIST SP 800-53, revision 4 recommends that organizations employ the principle of least privilege by allowing only authorized users (or processes acting on behalf of users) access permission that is necessary to accomplish assigned tasks in accordance with organizational missions and business functions. NIST also recommends periodic reviews of user accounts for compliance with account management requirements. In addition, FDIC policy requires administrators to use designated administrator accounts when conducting administrative tasks. FDIC policy also requires removal of user permissions if the job responsibilities of the user change, if the user transfers to a different organization, or the user no longer requires access for any other reason. Further, the policy requires that access settings be reviewed periodically to ensure that they remain consistent with existing authorizations and current business needs.

During 2016, FDIC improved controls for authorizing users' access by addressing all nine of the weaknesses pertaining to authorization that we had previously identified and that were still unresolved as of December 31, 2015.[15] For example, FDIC implemented processes for

- reviewing individuals with access to its data centers;
- ensuring that users of a key financial application do not conduct access reviews of their own accounts; and
- removing users' access to another financial application in a timely manner.

[15]The detailed findings and associated recommendations were communicated to FDIC in limited distribution reports in 2016 and 2015.

However, while it addressed these weaknesses from prior years, the corporation did not always consistently implement authorization controls. Specifically, FDIC database administrators for one database management system did not use designated administrative accounts when performing administrative tasks on certain databases. Additionally, although the corporation had a process for conducting periodic reviews of access settings on mainframe accounts, it did not include all mainframe accounts in the access review process. Further, about one-fifth of the user accounts we reviewed on a key financial application were granted additional privileges that had not been authorized by the users' supervisors. This occurred because the official granting the access had institutional knowledge of the privileges that the users would need, and because FDIC's procedures for granting access to the application did not include responsibilities and procedures for ensuring that the level of access provided had been approved by the users' supervisor. As a result, these systems are more vulnerable to unauthorized access and modification of data.

FDIC Did Not Employ Strong Encryption on Connections to Sensitive Mainframe Resources

Cryptography controls can be used to help protect the integrity and confidentiality of data and computer programs by rendering data unintelligible to unauthorized users and/or protecting the integrity of transmitted or stored data. Cryptography involves the use of mathematical functions called algorithms and strings of seemingly random bits called keys. Among other things, the algorithms and keys are used to encrypt a message or file so that it is unintelligible to those who do not have the secret key needed to decrypt it, thus keeping the contents of the message or file confidential. NIST SP 800-53, revision 4 recommends that organizations employ encryption to protect information from unauthorized disclosure and modification during transmission. The NIST standard for an encryption algorithm is Federal Information Processing Standards Publication (FIPS Pub.) 140-2.[16]

FDIC had not completed actions to implement our prior recommendation to use FIPS-compliant encryption for all mainframe connections.[17]

[16]NIST, *Security Requirements for Cryptographic Modules*, FIPS Pub. 140-2 (Gaithersburg, Md.: May 2001).

[17]The detailed finding and associated recommendation were communicated to FDIC in a limited distribution report in 2014.

Although FDIC officials stated that they initially intended to implement a tool to enable mainframe encryption in 2016, the corporation determined that the tool would not encrypt all of the information within its planned scope. FDIC officials from the Division of Information Technology stated that the corporation is continuing to consider feasible options for encrypting mainframe connections. In the meantime, sensitive data—such as user IDs and passwords—continue to be transmitted over the network in clear text, exposing them to potential compromise.

FDIC Did Not Scan All Servers for Vulnerabilities or Sufficiently Monitor Changes to Critical Files

Audit and monitoring involves the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the appropriate investigation and reporting of such activity. Automated mechanisms may be used to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. Audit and monitoring controls can help security professionals routinely assess computer security, perform investigations during and after an attack, and even recognize an ongoing attack.

NIST SP 800-53, revision 4 states that organizations should review and analyze information system audit records for indications of inappropriate or unusual activity and report the findings to designated agency personnel. Additionally, NIST states that information systems should produce audit records that establish the type of event, when the event occurred, and the identity of any individuals or subjects associated with the event, among other things.

FDIC improved its audit and monitoring controls by implementing four of the five recommendations pertaining to audit and monitoring that we had previously identified and that were still unresolved as of December 31, 2015.[18] For example, the corporation had

- ensured that data on successful logins was being captured for each of its database systems for investigation of potential security incidents;
- implemented a centralized audit monitoring capability for its databases;

[18]The detailed findings and associated recommendations were communicated to FDIC in limited distribution reports in 2016, 2014, and 2013.

- improved the logging and monitoring process for several key systems; and
- documented all critical files on key servers that required real-time monitoring.

However, other weaknesses existed in FDIC's implementation of audit and monitoring controls. Specifically:

- FDIC had not performed vulnerability scans of all servers in its IT environment. In its November 2016 report on the effectiveness of the corporation's information security program in accordance with the requirements of FISMA, the FDIC Office of Inspector General (OIG) reported that, at the time of its audit, FDIC was not performing vulnerability scans for more than 900 production servers within one of its general support systems.[19] In addition, we found that FDIC had not scanned several production servers in another of its general support systems during the 3-month time period (July, August, and September 2016) that we reviewed.

  According to FDIC officials, these conditions occurred because the corporation did not have an inventory of network assets that included all servers and because its legacy scanning and discovery tool had failed to identify all servers. The officials added that the scanning and discovery tool had since been replaced. Without regularly scanning all servers, FDIC cannot reasonably be assured that vulnerabilities in its servers are identified and corrected in a timely manner, increasing the risk that its systems and information may be compromised.

- FDIC had not completed actions to address our prior year recommendation to ensure that changes made to critical files on certain key servers are adequately monitored.[20] Although the corporation specified which directories on the servers were to be monitored, the logs that were generated did not provide sufficient detail to identify the individuals making changes.

[19]Federal Deposit Insurance Corporation, Office of Inspector General, *Audit of the FDIC's Information Security Program—2016*, AUD-17-001 (Arlington, Va.: November 2016). In a version of the report that was not made publicly available, the OIG made a recommendation related to this weakness.

[20]The detailed finding and associated recommendation were communicated to FDIC in a limited distribution report in 2016.

According to officials in FDIC's Division of Information Technology, the corporation plans to implement a new solution in 2017 to enable security personnel to identify users making file system changes. Until FDIC fully addresses this recommendation by ensuring that users making changes to critical files are identified and logged, increased risk continues to exist that an unauthorized individual could inappropriately modify these files without being identified.

FDIC Did Not Fully Implement Configuration Management Controls

In addition to access controls, agencies should implement policies, procedures, and techniques for managing the configuration of information systems. Configuration management controls are intended to prevent unauthorized changes to information system resources (for example, software programs and hardware configurations) and to provide reasonable assurance that systems are configured and operating securely and as intended. NIST SP 800-53, revision 4 recommends, among other things, that agencies develop and document an inventory of information system components that accurately reflects the current system and includes all components within the system's authorization boundary; establish a baseline configuration for the information system and its constituent components; and identify and correct information system flaws, including installing security relevant software updates within a defined time period of their release.

Consistent with NIST guidelines, FDIC policy states that mandatory configuration settings must be established and documented for IT products employed within the information system using information system-defined security configuration checklists. The policy also states that applicable vendor-released software patches designed to address security vulnerabilities are to be implemented in accordance with the CIO organization's security patching schedule.

Nevertheless, FDIC had not consistently implemented configuration management controls. For example, although the corporation used multiple tools to track and validate its IT assets, it had not established a single, authoritative, accurate listing of all IT assets in its environment. This occurred because FDIC had not established a process to reasonably assure that a complete, accurate inventory was developed and maintained. Additionally, although the corporation had defined baseline configuration settings for its information systems and had conducted

configuration scans of its systems, it had not yet fully implemented processes for verifying that configurations are consistently applied. Further, although FDIC had applied patches to certain third-party applications supporting financial processing and had made significant progress in identifying and tracking vulnerabilities related to third-party software, it had not yet fully implemented processes to ensure that assets that require patching are identified correctly.

Without establishing a reliable, authoritative listing of its IT assets and documenting, implementing, and monitoring security configurations, FDIC has reduced assurance that its information supporting financial processing is securely configured. Additionally, unless known vulnerabilities in FDIC's systems and applications are patched, increased risk exists that they could be exploited, potentially exposing the corporation's financial systems and information to unauthorized access or modification.

FDIC Developed and Documented Elements of Its Corporate Information Security Program, but Shortcomings Still Existed

An entitywide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied.

FISMA requires each agency to develop, document, and implement an information security program to provide security for the information and information systems that support the agency's operations and assets, including those provided or managed by another agency, contractor, or other organization on its behalf. Agency programs are to include, among other things, the following elements:

- periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;

- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency;
- policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each organizational information system;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization; and
- procedures for detecting, reporting, and responding to security incidents.

In addition, FISMA requires the head of each federal agency to ensure that information security management processes are integrated with agency strategic and operational planning processes.

FDIC had developed, documented, and implemented many elements of its corporate information security program. For example, it had

- defined security categories for the general support systems we reviewed based on risk using NIST guidance, assessed the risk from control deficiencies identified during security control tests, and ensured that the general support systems we reviewed were authorized to operate; and
- conducted a disaster recovery test of its general support systems and mission-critical applications.

However, FDIC had not fully or consistently implemented aspects of its information security program, which was an underlying reason for many

of the information security weaknesses identified during our review. Specifically, FDIC had not

- included all necessary information in procedures for granting access to a key financial application;
- fully addressed the FDIC OIG's finding that security control assessments of outsourced service providers had not been completed in a timely manner;
- fully addressed key previously identified weaknesses related to establishing agencywide configuration baselines and monitoring changes to critical server files; and
- completed actions to address the FDIC OIG's finding that the corporation had not ensured that major security incidents are identified and reported in a timely manner.

In addition, in November 2016, the FDIC OIG reported that the corporation had not yet developed and documented an up-to-date information security strategic plan or completed actions to address weaknesses in its Information Security Managers program. These shortcomings are discussed in more detail in the following section.

FDIC Developed Many Security Policies, but A Key Procedure Was Lacking

A key element of an effective information security program is to develop, document, and implement risk-based policies, procedures, and technical standards that govern the security over an agency's computing environment. Information security policy is essential to establishing roles, responsibilities, and requirements necessary for implementing an information security program. The supporting procedures provide the information and guidance on implementing the policies. According to NIST SP 800-53, revision 4, organizations should develop and document procedures to facilitate the implementation of access and configuration management policies and associated controls.

Although FDIC developed and documented many information security policies and procedures that were consistent with the NIST *Risk*

Management Framework,[21] its procedure for granting users access to a key financial application did not include responsibilities and steps for ensuring that the level of access provided had been approved by the users' supervisor. As a result, the official granting access to the application—who had institutional knowledge of the privileges that the users would need—granted additional privileges to some users for which they had not been previously approved. Until it updates its procedure to include these responsibilities and steps, FDIC will continue to face increased risk that users may be granted access to privileges in the application for which they have not been approved.

FDIC Assessed Security Controls, but Outsourced Service Providers Were Not Always Assessed Timely

A key element of an information security program is to test and evaluate policies, procedures, and controls to determine whether they are effective and operating as intended. Security control testing should include management, operational, and technical controls for every system identified in the agency's required inventory of major systems. Although control tests and evaluations may encourage compliance with security policies, the full benefits are not achieved unless the results are used to improve security. FISMA requires that the frequency of tests and evaluations of management, operational, and technical controls be based on risks and occur no less than annually.

The Office of Management and Budget (OMB) directs agencies to meet their FISMA-required controls testing by drawing on security control assessment results that include, but are not limited to, continuous monitoring activities. According to NIST SP 800-53, revision 4, continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. NIST also recommends that organizations monitor security control compliance by external service providers on an ongoing basis.

FDIC developed a continuous control assessment methodology that defined the controls tested for each information system and the frequency that each control is to be tested. In addition, the corporation tested the

[21]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (Gaithersburg, Md.: February 2010; updated June 2014).

effectiveness of the security controls for the three general support systems we reviewed in accordance with the methodology.

However, the FDIC OIG has previously reported weaknesses in FDIC's assessments of its outsourced service providers. Specifically, in October 2015, it reported that the corporation had not always ensured that security assessments of outsourced service providers were completed in a timely manner.[22] In November 2016, the OIG reported that FDIC had made meaningful progress towards completing timely assessments of its outsourced service providers, but noted that continued management attention was warranted in this area to ensure outstanding assessments are completed timely.[23]

FDIC Resolved Many Previously Identified Weaknesses, but Key Weaknesses Remain

When security weaknesses are identified, the related risks should be assessed, appropriate corrective or remediation actions should be taken, and follow-up monitoring should be performed to make certain that corrective actions are effective. FISMA specifically requires that agencywide information security programs include a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency.

NIST SP 800-53, revision 4 recommends that organizations develop a plan of action and milestones (POA&M) for information systems to document the planned remedial actions to correct weaknesses or deficiencies identified during security control assessments. A POA&M should also be updated based on the findings from the security controls assessment, security impact analysis, and continuous monitoring activities.

FDIC documented POA&Ms for weaknesses identified during internal control assessments and implemented an effective process for tracking and mitigating identified weaknesses for each of the systems that we

[22]FDIC, Office of Inspector General, *Audit of the FDIC's Information Security Program—2015*, AUD-16-001 (Arlington, Va.: October 2015). In a version of the report that was not made publicly available, the OIG made a recommendation related to this weakness.

[23]FDIC OIG, AUD-17-001.

reviewed. In addition, as of December 31, 2016, FDIC had addressed 15 of the 21 previously reported information system weaknesses that were unresolved at the end of our prior audit.[24] For example, FDIC had improved controls for authorizing users' access to financial applications and for logging and monitoring financial systems to detect potentially malicious activity. However, six previously identified weaknesses remained unresolved. Until it completes actions to address previously identified weaknesses, FDIC will continue to face increased risk that its systems may not be adequately or consistently protected against unauthorized access to systems or data. Appendix II details the status of weaknesses that were unaddressed as of December 31, 2015 or were initially reported in 2016.

Shortcomings Existed in FDIC's Incident Response Process

Comprehensive monitoring and incident response controls are necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. While strong controls may not prevent all incidents, agencies can reduce the risks associated with these events by detecting and promptly responding before significant damage is done. FISMA requires federal agencies to develop and implement procedures for detecting, reporting, and responding to security incidents. NIST SP 800-53, revision 4 further recommends that agencies develop, document, and disseminate procedures to facilitate the implementation of the incident response policy and associated incident response controls.

FDIC developed and documented information security policies and procedures on incident response. For example, its policy on reporting computer security incidents states that the FDIC Computer Security Incident Response Team is responsible for evaluating the seriousness of computer security incidents and taking appropriate corrective actions, including notifying FDIC senior management, the OIG, and other outside entities, when appropriate.

Nevertheless, shortcomings existed in FDIC's implementation of its policies. Specifically, FDIC did not provide reasonable assurance that

[24]GAO, *Information Security: FDIC Implemented Controls over Financial Systems, but Further Improvements Are Needed*, GAO-16-605 (Washington, D.C.: June 29, 2016).

"major incidents," as defined by OMB guidance,[25] were identified and reported in a timely manner. Specifically, the OIG reported in July 2016[26] that FDIC's incident response policies, procedures, and guidelines did not address major incidents. In addition, the large volume of potential security violations identified by its Data Loss Prevention tool, together with limited resources devoted to reviewing potential violations, hindered meaningful analysis of the information and FDIC's ability to identify all security incidents, including major ones. Among other things, the OIG recommended that FDIC (1) revise its incident response policies, procedures, and guidelines to address major incidents; (2) ensure that these revisions include criteria for determining whether an incident is major, consistent with FISMA and Office of Management and Budget guidance; and (3) review the current implementation of the Data Loss Prevention tool to determine how it can be better leveraged to safeguard sensitive FDIC information.

In November 2016, the FDIC OIG reported[27] that, in response to these findings, the corporation was working to improve its incident response capabilities by 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. If fully implemented, these actions could improve FDIC's ability to identify and address security incidents, including major incidents.

FDIC Did Not Complete Key Information Security Strategic Management Activities

According to NIST SP 800-39, effective risk management requires organizations such as FDIC to operate in highly complex, interconnected environments using state-of-the-art and legacy information systems—systems that organizations depend on to accomplish their missions and to conduct important business-related functions. The complex relationships among missions, mission/business processes, and the information

[25]OMB, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, M-16-03 (October 30, 2015).

[26]FDIC OIG, *The FDIC's Process for Identifying and Reporting Major Information Security Incidents*, AUD-16-004 (Arlington, Va.: July 2016).

[27]FDIC OIG, AUD-17-001.

systems supporting those missions and processes require an integrated, organization-wide view for managing risk.[28]

Effective management of information security risk is critical to the success of organizations in achieving their strategic goals and objectives. NIST SP 800-100 states that agencies should have a strategic plan for information security that identifies goals and objectives related to the agency's mission, specifies a plan for achieving those goals, and establishes short- and mid-term performance targets and measures that allow the agency to track, manage, and monitor its progress toward those goals and objectives.[29] In addition, according to NIST SP 800-39, agencies should establish roles and responsibilities for managing information security risk.

However, FDIC had not fully implemented key activities for managing and overseeing information security risk across the organization. Specifically:

- In November 2016, the FDIC OIG reported[30] that FDIC's information security strategic plan was not up-to-date. Specifically, although the corporation had an information security strategic plan, this plan had expired in 2015 and did not fully reflect OMB's cybersecurity priorities or the corporation's strategies. Without an up-to-date strategic plan, ongoing and planned IT initiatives may not be linked to the corporation's long-term security and business goals and priorities.
- FDIC had not completed actions to address gaps in how the roles and responsibilities of its Information Security Managers (ISM) are defined and carried out. In October 2015, the FDIC OIG reported[31] that the duties and roles of the ISMs in addressing information security requirements and risks had evolved since the ISM program was established. It also reported that FDIC had not completed a recent comprehensive assessment to determine whether the skills, training, oversight, and resource allocations pertaining to the ISMs enabled them to effectively carry out their increased responsibilities and

[28]NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, Md.: March 2011).

[29]NIST, *Information Security Handbook: A Guide for Managers*, SP 800-100 (Gaithersburg, Md.: October 2006).

[30]FDIC OIG, AUD-17-001. In a version of the report that was not made publicly available, the OIG made a recommendation related to this weakness.

[31]FDIC OIG, AUD-16-001. In a version of the report that was not made publicly available, the OIG made a recommendation related to this weakness.

address security risks within their divisions and offices. In November 2016, the OIG reported that FDIC had conducted an assessment of its ISM program, which identified gaps in areas such as available resources, training, and performance measurement. The OIG also reported that FDIC plans to complete all actions to address these gaps by 2018. Until then, however, increased risk exists that these capability gaps could impact the effectiveness of the FDIC's information security program.

Conclusions

FDIC had implemented and strengthened many information security controls over its financial systems and information. For example, the corporation had taken steps to improve controls for restricting user access to only what has been authorized, auditing and monitoring systems for potentially malicious activity, and applying patches to address known software vulnerabilities by addressing many of the weaknesses that we previously reported. However, management attention is needed to address new and previously identified deficiencies in access controls—including boundary protection, identification and authentication, authorization, cryptography, and audit and monitoring controls—and in configuration management controls. These deficiencies, considered collectively, are the basis for our determination that FDIC had a significant deficiency in internal control over financial reporting in its information systems controls as of December 31, 2016.

In addition, FDIC had developed, documented, and implemented many elements of its corporate information security program. However, further actions are needed to address shortcomings in the corporation's program, such as ensuring that its procedure for granting access to a key financial application includes key responsibilities and steps.

Given the important role that information systems play in FDIC's internal controls over financial reporting, it is vitally important that the corporation address weaknesses in information security controls—both old and new—as part of its ongoing efforts to mitigate the risks from cyber attacks and to ensure the confidentiality, integrity, and availability of its financial and sensitive information. Continued and consistent management commitment and attention to access, configuration management, and security management controls will be essential to addressing existing deficiencies and further improving FDIC's information system controls.

Recommendations for Executive Action

To help improve the corporation's implementation of its information security program, we recommend that the Chairman of FDIC direct the Chief Information Officer to update the procedure for granting access to the key financial application, to include responsibilities and steps for ensuring that the access privileges granted have been approved by the users' supervisor.

In a separate report with limited distribution, we are also making six recommendations to resolve shortcomings in FDIC's internal control over financial reporting and help strengthen access and configuration management controls over key financial information, systems, and networks.

Agency Comments and Our Evaluation

In written comments on a draft of this report (reprinted in appendix II), FDIC concurred with our recommendation to improve its implementation of its information security program and stated that corrective actions will be completed by July 2017. FDIC also provided an attachment detailing its actions to implement our recommendation.

In addition to the aforementioned comments, FDIC provided technical comments that we have addressed in our report as appropriate. In these comments, the corporation expressed concern about one additional recommendation to improve its information security program that we had made in our draft report. Specifically, the draft report had included a recommendation that FDIC develop, document, and implement procedures for ensuring that configuration actions identified by its Computer Security Incident Response Team are taken. In written and oral comments, FDIC officials provided additional information about the corporation's incident handling process in order to clarify that the condition we identified did not pose a risk to the corporation's information and systems. After our review of this information, we agree that the condition does not pose a risk to the corporation and, accordingly, removed the recommendation from our final report.

We are sending copies of this report to interested congressional parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you have any questions regarding this report, please contact Nick Marinos at (202) 512-9342 or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at marinosn@gao.gov and barkakatin@gao.gov. Key contributors to this report are listed in appendix II.

Nick Marinos
Director, Information Technology

Dr. Nabajyoti Barkakati
Director, Center for Science, Technology, and Engineering

Appendix I: Objective, Scope, and Methodology

The objective of this information security review was to determine the effectiveness of the Federal Deposit Insurance Corporation's (FDIC) controls in protecting the confidentiality, integrity, and availability of its financial systems and information. To do this, we identified and reviewed FDIC information systems control policies and procedures, tested controls over key financial applications, and held interviews with key security representatives and management officials in order to determine whether information security controls were in place, adequately designed, and operating effectively. The review was conducted as part of our audit of the financial statements of the two funds administered by FDIC: the Deposit Insurance Fund and the Federal Savings and Loan Insurance Corporation Resolution Fund.

The scope of our audit included an examination of FDIC information security policies, procedures, and controls over key financial systems in order to (1) assess the effectiveness of corrective actions taken by FDIC to address weaknesses we previously reported and (2) determine whether any additional weaknesses existed. This work was performed in support of our opinion on internal control over financial reporting as it relates to our audits of the calendar years 2016 and 2015 financial statements of the two funds administered by FDIC.

The independent public accounting firm of Cotton & Company LLP tested certain FDIC information systems controls, including the follow-up on the status of FDIC's corrective actions during calendar year 2016 to address open recommendations from our prior years' reports. We agreed on the scope of the audit work, monitored the firm's progress, and reviewed the related audit documentation to determine whether the firm's findings were adequately supported.

To determine whether controls over key financial systems and information were effective, we considered the results of FDIC's actions to mitigate previously-reported weaknesses that remained open as of December 31, 2015, and performed audit work at FDIC facilities in Arlington, Virginia. We concentrated our evaluation primarily on the controls for systems and applications associated with financial processing, such as the (1) New Financial Environment; (2) Communication, Capability, Challenge, and Control System; (3) Portfolio Investment Accounting; (4) Assessments

Information Management System; and (5) general support systems. Our selection of the systems to evaluate was based on consideration of systems that directly or indirectly support the processing of material transactions that are reflected in the funds' financial statements.

Our audit methodology was based on the *Federal Information System Controls Audit Manual*,[1] which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information.

Using standards and guidance from the National Institute of Standards and Technology and the Office of Management and Budget, as well as FDIC's policies and procedures, we evaluated controls by

- examining network diagrams and device configuration settings to determine if intrusion detection and prevention systems were monitoring the FDIC network for suspicious activity;
- reviewing privileged accounts to verify that access to privileged accounts was appropriately controlled and that accounts were not shared among multiple users;
- analyzing user application authorizations to determine whether users had more permissions than necessary to perform their assigned functions;
- reviewing administrative account settings to determine if privileged accounts were used as required and if access to a privileged account was appropriately controlled;
- assessing configuration settings to evaluate settings used to audit security-relevant events; and
- inspecting vulnerability scans for in-scope systems to determine whether scans were conducted regularly and whether patches were appropriately installed on affected systems.

Using the requirements of the *Federal Information Security Modernization Act of 2014*, which establishes elements for an agency-wide information security program, we evaluated FDIC's implementation of its security program by

[1]GAO, *Federal Information System Controls Audit Manual*, GAO-09-232G (Washington, D.C.: Feb. 2, 2009)

- examining system authorization documentation for information on FDIC's implementation of risk categorization and risk assessment practices;
- reviewing information security policies and procedures to determine whether they were adequately documented and implemented;
- examining FDIC training records for information on general and specialized training;
- reviewing assessments of security controls to determine if they had been completed as scheduled;
- reviewing an FDIC Office of Inspector General (OIG) report for information on the corporation's processes for assessing security controls of outsourced service providers;
- examining remedial action plans to determine whether FDIC had addressed identified vulnerabilities in a timely manner;
- examining two FDIC OIG reports for information on the corporation's incident response process;
- reviewing security event records to determine if security events were tracked and resolved appropriately;
- reviewing continuity of operations plans, contingency plans, and test results to determine whether contingency planning controls were appropriately implemented; and
- examining two FDIC OIG reports for information on the corporation's information security strategic management activities.

To determine the status of FDIC's actions to correct or mitigate previously reported information security weaknesses, we reviewed prior GAO reports to identify previously reported weaknesses, examined FDIC's corrective action plans, and assessed the effectiveness of those actions.

We conducted this audit in accordance with U.S. 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 objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the Federal Deposit Insurance Corporation

FDIC
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Deputy to the Chairman and CFO

May 19, 2017

Mr. Nick Marinos
Director, Information Technology
Dr. Nabajyoti Barkakati
Director, Center for Science, Technology, and Engineering
U.S. Government Accountability Office
Washington, D.C. 20548

Dear Mr. Marinos and Dr. Barkakati:

Thank you for the opportunity to comment on the U.S. Government Accountability Office's (GAO's) draft audit report titled, Information Security: FDIC Needs to Improve Controls over Financial Systems and Information; GAO-17-436. We appreciate GAO's identification of opportunities to improve information security as well as GAO's acknowledgement of security improvements FDIC implemented in the past year. FDIC recognizes the important role a strong information security program plays in maintaining good fiscal management and remains dedicated to strengthening this area of its operations. FDIC management and staff will focus additional attention on information security during the upcoming year.

The GAO's report contains one recommendation to help the FDIC improve implementation of its information security program. Corrective action will be completed by July 2017 for this recommendation. FDIC response details are included in Attachment 1.

Once again, we thank you for your past contributions and your work on this year's audit. We look forward to continuing our dialogue on actions planned and performed to address recommendations from the current year and prior year audits that GAO reported as not being fully resolved at the completion of fieldwork. If you have any questions relating to the FDIC management response, please contact Craig Jarvill, Director, Division of Finance, at 703-562-6206.

Sincerely,

Steven O. App
Deputy to the Chairman and
Chief Financial Officer

Attachment
cc: Lawrence Gross, Jr.
Craig Jarvill
Arleas Upton Kea
Audit Committee

Attachment 1

FDIC RESPONSE DETAILS

Procedure Enhancement
Update the procedure for granting access to the key financial application, to include responsibilities and steps for ensuring that the access privileges granted have been approved by the users' supervisor.
Recommendation 1 – Concur; Expected Completion Date 07/31/2017
Procedures will be revised to reflect the updated practice for granting access to the key financial application, to include responsibilities and steps for ensuring that the access privileges granted have been approved by the user's supervisor.

Page 1

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nick Marinos, (202) 512-9342, marinosn@gao.gov

Dr. Nabajyoti Barkakati, (202) 512-4499, barkakatin@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Gregory Wilshusen (Director); Gary Austin, Paul Foderaro, and Michael Hansen (Assistant Directors); William Cook (Analyst in Charge); Wayne Emilien; Nancy Glover; Franklin Jackson; Thomas J. Johnson; Jean Mathew; David Plocher; Dacia Stewart; and Adam Vodraska made key contributions to this report.

Appendix IV: Accessible Data

Agency Comment Letter

Text of Appendix II: Comments from the Federal Deposit Insurance Corporation

Page 1

May 19, 2017

Mr. Nick Marinos

Director, Information Technology

Dr. Nabajyoti Barkakati

Director, Center for Science, Technology, and Engineering

U.S. Government Accountability Office Washington, D.C. 20548

Dear Mr. Marinos and Dr. Barkakati:

Thank you for the opportunity to comment on the U.S. Government Accountability Office's (GAO's) draft audit report titled, Information Security: FDIC Needs to Improve Controls over Financial Systems and Information; GA0-17-436. We appreciate GAO's identification of opportunities to improve information security as well as GAO's acknowledgement of security improvements FDIC implemented in the past year. FDIC recognizes the important role a strong information security program plays in maintaining good fiscal management and remains dedicated to strengthening this area of its operations.

FDIC management and staff will focus additional attention on information security during the upcoming year.

The GAO's report contains one recommendation to help the FDIC improve implementation of its information security program. Corrective action will be completed by July 2017 for this recommendation. FDIC response details are included in Attachment 1.

Once again, we thank you for your past contributions and your work on this year's audit. We look forward to continuing our dialogue on actions planned and performed to address recommendations from the current year and prior year audits that GAO reported as not being fully resolved at the completion of fieldwork. If you have any questions relating to the FDIC management response, please contact Craig Jarvill, Director, Division of Finance, at 703-562-6206.

Sincerely,

Steven 0. App

Deputy to the Chairman and Chief Financial Officer

Attachment

cc: Lawrence Gross, Jr.

Craig Jarvill Arleas Upton Kea Audit Committee

Page 2

Procedure Enhancement

Update the procedure for granting access to the key financial application, to include responsibilities and steps for ensuring that the access privileges granted have been approved by the users' supervisor.

Recommendation 1 - Concur; Expected Completion Date 07/31/2017

Procedures will be revised to reflect the updated practice for granting access to the key financial application, to include responsibilities and steps for ensuring that the access privileges granted have been approved by the user's supervisor.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548