



June 2016

INFORMATION SECURITY

FDIC Implemented
Controls over
Financial Systems,
but Further
Improvements Are
Needed

GAO Highlights

Highlights of [GAO-16-605](#), 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 2015 financial statements of the Deposit Insurance Fund and the Federal Savings and Loan Insurance Corporation Resolution Fund 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

In addition to the 9 prior recommendations that have not been fully addressed, GAO is making 2 recommendations to improve FDIC's implementation of its information security program. In a separate report with limited distribution, GAO is making 10 new recommendations to FDIC to address newly-identified weaknesses in access controls. FDIC concurred with GAO's recommendations.

View [GAO-16-605](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

June 2016

INFORMATION SECURITY

FDIC Implemented Controls over Financial Systems, but Further Improvements are Needed

What GAO Found

The Federal Deposit Insurance Corporation (FDIC) has implemented numerous information security controls intended to protect its key financial systems; however, weaknesses remain that place the confidentiality, integrity, and availability of financial systems and information at risk. During calendar year 2015, the corporation continued to devote attention to securing its financial information and systems that support its mission. Key among its actions were improving controls for identifying and authenticating the identity of users and improving controls for authorizing users' access. However, FDIC continues to have unremediated weaknesses. For example, the corporation (1) did not have an effective process for recertifying user access rights to several systems supporting the corporation's financial processing and (2) had not yet applied critical patches to mitigate known vulnerabilities in third party software on systems supporting financial processing.

Although the corporation had a comprehensive framework for its information security program, some aspects were not fully implemented. For example, the corporation did not (1) fully document and implement procedures for performing system access requests, assignments, and removal and (2) have a policy for monitoring critical file changes. In addition, FDIC had yet to fully address 9 previously-reported weaknesses that were unresolved as of December 31, 2014, as indicated in the following table.

Status of GAO Information Security Recommendations to FDIC as of December 2015

Information security control area	Prior GAO recommendations open at the start of calendar year 2015 audit	Recommendations closed during calendar year 2015 audit	Outstanding prior recommendations at the end of calendar year 2015 audit
Information security program		2 (2)	0
Access controls	10	(5)	5
Other controls	4	(0)	4
Total	16	(7)	9

Source: GAO analysis of FDIC data. | GAO-16-605

While newly-identified weaknesses, along with those previously identified that remain uncorrected, are not individually or collectively a material weakness or a significant deficiency for financial reporting purposes, the corporation will have limited assurance that its sensitive financial information and resources will be secure until these weaknesses have been mitigated.

Contents

Letter		1
	Background	2
	FDIC Continued to Make Progress in Addressing Control Weaknesses, but Further Improvements Are Needed	6
	Conclusions	16
	Recommendations for Executive Action	16
	Agency Comments	16
Appendix I	Objective, Scope, and Methodology	18
Appendix II	Comments from the Federal Deposit Insurance Corporation	21
Appendix III	GAO Contacts and Staff Acknowledgments	24

Abbreviations

4C	Communication, Capability, Challenge, and Control system
CHRIS T&A	Corporate Human Resources Information System Time & Attendance
CIO	chief information officer
FDIC	Federal Deposit Insurance Corporation
FIPS Pub.	<i>Federal Information Processing Standards Publication</i>
FISMA	<i>Federal Information Security Modernization Act of 2014</i> <i>Federal Information Security Management Act of 2002</i>
IAMS	Identity Access Management System
NFE	New Financial Environment
OIG	Office of the Inspector General
NIST	National Institute of Standards and Technology
PORTIA	Portfolio Investment Accounting
RRPS	Risk Related Premium System
SP	Special Publication

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



June 29, 2016

The Honorable Martin J. Gruenberg
Chairman
Federal Deposit Insurance Corporation

Dear Chairman Gruenberg:

The Federal Deposit Insurance Corporation (FDIC) has a demanding responsibility enforcing banking laws, regulating banking institutions, and protecting depositors. In carrying out its financial and mission-related operations, the corporation relies extensively on computerized systems. Because it plays an important role in maintaining public confidence in the nation's financial system, 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 its 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 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. In our financial audit report,¹ we concluded that FDIC maintained, in all material respects, effective internal control over financial reporting as of December 31, 2015, based on criteria established under the *Federal Managers' Financial Integrity Act of 1982*.²

Our objective was to determine the effectiveness of the corporation's 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, 2015.

¹GAO, *Financial Audit: Federal Deposit Insurance Corporation Funds' 2015 and 2014 Financial Statements*, [GAO-16-300](#) (Washington, D.C.: February 2016).

²31 U.S.C. § 3512(c) and (d).

We performed our work 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 provided a reasonable basis for our findings and conclusions based on our audit objective. See appendix I for more details on our objective, scope, and methodology.

Background

FDIC was created 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 1933³ in response to the thousands of bank failures that had occurred throughout the late 1920s and early 1930s.⁴ FDIC identifies, monitors, and addresses risks to the Deposit Insurance Fund when a bank or thrift institution fails.

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.⁵ The act also designated FDIC as the administrator of the Federal Savings and Loan Insurance Corporation Resolution Fund, which 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.⁶ The Bank Insurance Fund and the Savings Association Insurance Fund merged into the Deposit Insurance

³*Federal Deposit Insurance Corporation Act*, June 16, 1933, Ch. 89, § 8.

⁴FDIC 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.

⁵Pub. L. No. 101-73, § 211, 103 Stat. 183, 218-22 (Aug. 9, 1989).

⁶A 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, 124 Stat. 1376, 1506 (July 21, 2010), is unfunded and conducted no transactions during the fiscal years covered by this audit.

Fund on February 8, 2006, as a result of the passage of the *Federal Deposit Insurance Reform Act of 2005*.⁷

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 and a layered approach to information security defense.

To support its financial management functions, FDIC uses, among others, the following 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 Corporation⁸ interest amounts from insured institutions;
- a Web-based application that provides full functionality to support franchise marketing,⁹ 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;¹⁰

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

⁸The 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.

⁹Franchise marketing is a process where the FDIC markets troubled institutions to healthy insured depository institutions to help maintain financial system stability and public confidence.

¹⁰Under 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.

Cyber Threats Facing Federal Systems Continue to Evolve

- 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.

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 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.

Recent security incidents at FDIC highlight these threats. In May 2016, FDIC's Chief Information Officer (CIO) testified about separate incidents involving the removal of personally identifiable information and other sensitive information by FDIC personnel using portable media shortly before their separation from the corporation. It was the CIO's initial judgment that these incidents did not rise to the level of "major incident" as defined in the OMB guidance. However, the Office of Inspector General (OIG) reviewed one of these incidents and came to a different conclusion. The OIG, in a memorandum dated February 19, 2016, recommended that the incident they reviewed be reported to Congress under the category of "major incident." Subsequently, the corporation elevated the incident to a "major incident" and reported this to Congress 7 days later.

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),¹¹ 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 CIO the authority to ensure compliance with the requirements imposed on the agency under FISMA.

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. The CIO also serves as the authorizing official with the authority to approve the operation of the information systems at an acceptable level of risk to the corporation.

The Chief Information Security Officer reports to the CIO and serves as his designated representative. According to the corporation's policy, Chief Information Security Officer is responsible for (1) the overall support of assessment and authorization activities; (2) the development, coordination, and implementation of FDIC's security policy; and (3) the coordination of information security and privacy efforts across the corporation.

¹¹The *Federal Information Security Modernization Act of 2014* (FISMA 2014), 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 FISMA 2014, FISMA 2002 requirements relevant here that were incorporated and continued in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

FDIC Continued to Make Progress in Addressing Control Weaknesses, but Further Improvements Are Needed

Although FDIC has designed and documented numerous information security controls intended to protect its key financial systems and data, several of these information security controls were not consistently documented or implemented. Additionally, FDIC developed and documented many elements of its information security program. However, the corporation did not always consistently implement key information security program activities. By mitigating known information security weaknesses and ensuring that information security controls are consistently applied, FDIC could continue to reduce risks and better protect its sensitive financial information and resources from inadvertent or deliberate misuse, improper modification, unauthorized disclosure, or destruction.

Numerous Access Controls Were Implemented, but Shortcomings Require Management Attention

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 identifying and authenticating users, restricting user access to only those users with a business need, encrypting sensitive data, auditing and monitoring systems to detect potentially malicious activity, managing and controlling system configurations, and conducting employee background investigations, among other things. Although FDIC had implemented numerous controls in these areas, weaknesses continue to challenge the corporation in ensuring the confidentiality, integrity, and availability of its information and information systems.

Identification and Authentication Controls Were Improved

Information systems need to effectively control user accounts and identify and authenticate users. Users and devices should be appropriately identified and authenticated through the implementation of adequate logical access controls. Users can be authenticated using mechanisms such as a password and user identification combination. National Institute of Standards and Technology (NIST) guidance¹² recommends that agency information systems enforce minimum password complexity requirements. Accordingly, FDIC policy requires passwords to be at least eight characters in length.

¹²National Institute of Science and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, revision 4 (Gaithersburg, Md.: April 2013).

Results of Periodic Reviews
Were Not Consistently Acted
On

FDIC improved controls for identifying and authenticating the identity of users by implementing its policy on password controls over the Portfolio Investment Accounting (PORTIA) application. As a result, FDIC has reduced its risk that passwords could potentially be compromised and used to gain unauthorized access to financial information in the application.

Authorization encompasses access privileges granted to a user, program, or process. It is used to allow or prevent actions by that user based on predefined rules. Authorization includes the principles of legitimate use and least privilege.¹³ 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; periodically review the privileges assigned to users to validate the need for such privileges, and reassign or remove privileges when necessary; and disable access to information systems within a defined period when individuals are terminated.

Consistent with NIST guidance, FDIC policy states that access to IT resources shall be terminated after an employee or contractor exits the FDIC and that periodic reviews of access settings shall be conducted to ensure that appropriate controls remain consistent with existing authorizations and current business needs.

During 2015, FDIC improved controls for authorizing users' access. For example, FDIC had implemented

- policies and procedures to ensure that network access is removed in a timely manner when a user is separated from FDIC,
- procedures to document reviews of user access to a system supporting the marketing of failed banks, and
- procedures to ensure that all user accounts are included in the periodic reviews of user access to resources supporting financial processing.

¹³Users should have the least amount of privileges (access to services) necessary to perform their duties.

Although FDIC strengthened authorization controls by implementing most of the unresolved recommendations, the corporation did not

- have an effective process for performing periodic reviews of user access rights for several systems supporting the corporation's financial processing,
- consistently disable accounts belonging to users who had not accessed a financial system in a predefined period of time,
- consistently document that modifications to user access to systems had been authorized before making the changes, and
- identify authorization and recertification deficiencies during its oversight of an outsourced system.

While these weaknesses did not materially impact FDIC's financial statements, they nevertheless increase the risk that individuals may have greater access to financial data or to assets supporting financial processing than they need to fulfill their responsibilities.

Encryption for Sensitive Connections Had Not Yet Been Implemented

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 to, among other things, 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 guidance states that the use of encryption by organizations can reduce the probability of unauthorized disclosure of information. NIST also states that organizations should use cryptography to prevent unauthorized disclosure of information during transmission and encrypt passwords in storage and in transmission. The NIST standard for an encryption algorithm is *Federal Information Processing Standards Publication* (FIPS Pub.) 140-2.¹⁴

While FDIC established a project plan for implementing encryption, it had not implemented and used FIPS-compliant encryption for all mainframe connections. As a result, sensitive data—such as user IDs and

¹⁴National Institute of Science and Technology, *Security Requirements for Cryptographic Modules*, FIPS Pub. 140-2 (Gaithersburg, Md.: May 2001).

passwords—continue to be transmitted over the network in clear text, exposing them to potential compromise.

Effective Audit and Monitoring Controls Were Not Always Fully Implemented

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 guidance 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 officials. Additionally, NIST states that information systems should produce audit records that sufficiently describe the nature of events.

FDIC improved its audit and monitoring controls by ensuring that log data for three systems supporting financial processing were sent to the centralized logging system.

However, FDIC did not always effectively monitor server security logs and changes to a server's critical files. Specifically, FDIC had not documented, within its policies and procedures, which critical files should be monitored for changes. Additionally, it had not ensured that, for certain systems, sensitive and high risk events are consistently logged and audit logs are consistently reviewed.

While these weaknesses did not materially affect the corporation's financial statements, they nevertheless increase the risk that the incident response team would not detect malicious activity occurring on these systems supporting financial processing in a timely manner. Further, sufficient data may not be available that may hinder efforts to review potential security incidents in real time.

Procedures for Controlling Physical Access to Facilities Were Not Always Fully Implemented

Physical security controls restrict physical access or harm to computer resources and protect these resources from intentional or unintentional loss or impairment. NIST recommends that organizations develop, approve, and maintain a list of individuals with authorized access to facilities where information systems reside, periodically review the list, and remove individuals from the list when access to the facility is no longer required.

Corporation Had Not Fully Implemented Key Configuration Management Controls

While the corporation had updated its physical access policies to require periodic review of access to FDIC data centers, the corporation had not completed actions to effectively perform the recertification of individuals with physical access to its data centers. Additionally, although FDIC began conducting periodic reviews, access for four individuals was not removed in a timely manner following one such review. Access request forms had not been completed for 13 of 28 individuals in our sample whose access was granted in 2015. As a result, increased risk exists that unauthorized individuals may have access to sensitive FDIC resources.

Configuration management is an important control that involves the identification and management of security features for all hardware and software components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. Configuration management involves, among other things, (1) verifying the correctness of the security settings in the operating systems, applications, or computing and network devices and (2) obtaining reasonable assurance that systems are configured and operating securely and as intended. NIST SP 800-53, revision 4 states that organizations should establish a baseline configuration for the information system and its constituent components. Consistent with NIST guidelines, corporation 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.

Patch management, a component of configuration management, is important for mitigating the risks associated with software vulnerabilities. When a vulnerability is discovered, the software vendor may develop and distribute a patch or work-around to mitigate the vulnerability, and the customer is to install it as soon as possible. If the customer does not do so, an attacker can exploit the vulnerability to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other systems. NIST SP 800-128¹⁵ states that organizations should define the patch management process and how it is integrated into configuration management processes, how patches are prioritized and approved

¹⁵National Institute of Science and Technology, *Guide for Security-Focused Configuration Management of Information Systems*, SP 800-128 (Gaithersburg, Md.: August 2011).

through the configuration change control process, and how they are tested for their impact on existing secure configurations.

FDIC has not fully established configuration baselines or applied security patches in a timely manner to systems supporting financial processing. Specifically,

- The corporation had not completed actions to fully establish baseline configurations for its platforms which support financial systems, including documenting mandatory configuration settings and creating security configuration checklists. While the corporation has created baselines, it has not yet completed implementation and monitoring of all information systems.
- FDIC had begun to implement actions intended to improve its process for managing vulnerabilities and applying patches, including establishing a Patch and Vulnerability Group to facilitate the identification and distribution of patches. However, the corporation had not yet fully implemented procedures for applying patches, including critical patches, to remediate known vulnerabilities in third party software on systems supporting financial processing.

While these issues did not materially affect the corporation's financial statements, they nevertheless increase the risk that unpatched vulnerabilities in systems and applications could be exploited, potentially exposing the corporation's financial systems and information to unauthorized access or modification.

FDIC Has Yet to Complete Efforts to Perform Employee Background Reinvestigations

Following policies for hiring and retaining personnel is important in retaining employees who have adequate security clearances for the jobs to which they are assigned. Hiring and retention procedures should include performing background investigations and ensuring that periodic reinvestigations are consistent with the sensitivity of the position, in accordance with criteria from the Office of Personnel Management.

Current FDIC policy states that personnel in moderate- and low-risk positions should be subject to a background reinvestigation every 5 and 7 years, respectively. FDIC officials stated that efforts are underway to update the policy to eliminate the requirement to perform reinvestigations for employees in low-rated security positions in order to be consistent with current Office of Personnel Management guidance. In addition, FDIC plans to address our previous recommendation to perform background investigations consistent with this new policy by July 2016 and will include

reinvestigations for all employees in moderate-rated security positions. Until this weakness is addressed, FDIC continues to face an increased risk that it will not identify users who should not have access to sensitive systems.

Many Information Security Program Activities Were Implemented, but Further Improvements Are Needed

A key reason for the information security weaknesses in FDIC's financial systems was that, although the corporation had a comprehensive framework for its information security program, some aspects were not fully implemented.

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 that, among other things, includes

- 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;
- 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;
- provide specialized training to personnel with significant security responsibilities;
- 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; and

-
- 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.

FDIC had made improvements in developing and documenting many elements of its corporate information security program. For example, during 2015,

- The OIG reported that the FDIC had revised its corporate information security risk management program policy to better align with NIST guidance.
- FDIC had taken steps to improve its information security policies by updating policies to require that the continued need for access be periodically reviewed for the access rights of personnel with access to its data centers. In addition, the corporation had updated its policies to require that verifications of user access to a system supporting the marketing of failed banks' assets be documented.
- The corporation had addressed the OIG's recommendation to develop and approve a corporate-wide information security continuous monitoring strategy consistent with Office of Management and Budget and NIST guidance.¹⁶ If properly implemented, FDIC can gain better assurance that it will more effectively assess, communicate, and respond to emerging security threats, vulnerabilities, and issues.
- FDIC improved its process for managing known security weaknesses through development and use of a plan of actions and milestones.

Although FDIC continued to improve implementation of its corporate information security program, shortcomings existed in several information security program elements. Specifically,

- The corporation had not consistently managed risks identified during assessments of outsourced information service providers. The OIG reported in 2015 that FDIC did not have a standard mechanism in place to capture the risks identified during the assessments and communicate those risks to corporate leadership.¹⁷ It recommended

¹⁶Federal Deposit Insurance Corporation, Office of Inspector General, *Audit of FDIC's Information Security Program—2015*, AUD-16-001 (Arlington, VA: October 2015).

¹⁷AUD-16-001.

that the corporation implement a process for capturing risks and presenting them to management on a regular basis. FDIC concurred with the OIG and stated it would assess the Information Security Manager methodology to identify any needed improvements (particularly with regard to timeliness) by June 30, 2016. The assessment will contain a plan of action to implement any needed improvements. The OIG noted that this process should be integrated with the risk management processes already in place, such as the plans of action and milestones process. Without such a process, leadership may have limited access to information from its outsourced information service provider assessments, potentially leaving it exposed to risks that it would not normally accept.

- FDIC had not fully developed and documented procedures for performing system access requests, assignments, and removal in order to facilitate effective review or verification of users' system access privileges. The corporation created a policy that states that access should be (1) granted only for legitimate business use and only after proper authorization has been provided and (2) removed if the user no longer requires access. However, it had not established procedures to ensure that authorizations for the removal or modification of system access rights was consistently documented and performed in a timely manner following the periodic review of user privileges. Without establishing and implementing such procedures, officials may be inconsistent in their reviews and/or removal of access permissions in a timely manner. Therefore, increased risk exists that a user could have access to accounts or roles that are not necessary for job duties. Corporation officials acknowledged that improvements are needed in its procedures for ensuring timely removal of access as part of the recertification process.
- FDIC did not have a policy in place to require and govern the monitoring of changes to critical files used to configure security and access on servers. According to NIST, changes made to critical files should be monitored due to the high security impact they could have within an information systems environment. However, the corporation had not documented within policies which critical files should be monitored and how often. According to FDIC personnel, FDIC has a product in place that was logging critical files and sending alerts. When FDIC changed products for monitoring of these critical files, it had not configured specific alerts based on the use cases, nor conducted near real-time analysis of those changes. Until FDIC develops, documents, and implements a policy that identifies critical files for monitoring, its management is at increased risk that it may not

be made aware of changes to critical files as they occur. This may impact the ability of the corporation to react in a timely manner to potential security incidents and increases the risk that potential security events go undetected.

- FDIC had not completed an assessment related to the skills and training of its information security managers. Specifically, the OIG reported in 2015 that the role and duties of FDIC's Information Security Manager in addressing information security requirements and risks within the FDIC's business divisions and offices have evolved since the information security management program was established.¹⁸ However, the corporation has not completed a comprehensive assessment to determine whether the skills, training, oversight, and resource allocation pertaining to its information security managers will enable them to effectively carry out their increased responsibilities and address security risks within their divisions and offices. Therefore, the OIG recommended that the corporation develop a comprehensive plan to assess the role of an information security manager in managing information security risks within the divisions and offices. The corporation concurred with the recommendation. Absent this comprehensive assessment of the role, the corporation has reduced assurance that it can effectively address the risks associated with a rapidly changing threat environment.
- FDIC had not yet fully addressed several weaknesses that we previously identified in its information systems supporting financial processing. During 2015, FDIC had resolved 7 of the 16 previously-reported security weaknesses that were unresolved as of December 31, 2014. However, FDIC had not fully resolved 9 previously-reported weaknesses including three relating to authorization, audit and monitoring, and configuration management, among others.

¹⁸According to the Inspector General's report, the FDIC designed its information security management program to ensure an enterprise-wide approach to information security. The information security managers provide a security focus within their respective divisions and offices and are tasked with working to educate employees and contractors who have access to corporate systems and data.

Conclusions

FDIC made improvements in developing and documenting many elements of its corporate information security program. However, security controls were not always consistently implemented. Specifically, the corporation did not (1) fully document and implement procedures for performing system access requests, assignments, and removal or (2) have a policy for monitoring critical security file changes. Given the role that information systems play in FDIC's internal controls over financial reporting, it is important that the corporation address the remaining weaknesses in information security controls that we and the Office of Inspector General identified—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. Although we do not consider these weaknesses individually or collectively to be either a material weakness or a significant deficiency for financial reporting purposes, the corporation will have limited assurance that its sensitive financial information and resources will be secure until these weaknesses have been mitigated.

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 take the following actions:

- Update and implement access control procedures to require that authorizations for the removal or modification of access rights are documented and that approved changes are acted on in a timely manner.
- Develop and implement a policy that requires monitoring changes to critical files for the platforms identified during the audit.

In a separate report with limited distribution, we are also making ten detailed recommendations consisting of actions to be taken to correct specific information security weaknesses related to access control and audit and monitoring.

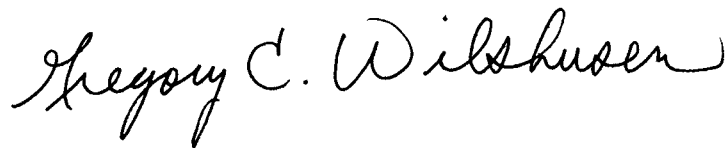
Agency Comments

In a letter providing written comments (reprinted in app. II) on a draft of this report, FDIC's Deputy to the Chairman and Chief Financial Officer stated FDIC concurred with our two recommendations to improve FDIC's implementation of its information security program and that corrective actions for the two new recommendations will be completed during 2016.

FDIC also provided technical comments that we addressed in our report as appropriate.

We are also sending copies of this report to interested congressional parties.

If you have any questions regarding this report, please contact Gregory C. Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at wilshuseng@gao.gov and barkakatin@gao.gov. Key contributors to this report are listed in appendix III.



Gregory C. Wilshusen
Director, Information Security Issues



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 assess information systems controls, we identified and reviewed FDIC information systems control policies and procedures, conducted tests of their controls, and held interviews with key security representatives and management officials concerning whether information security controls were in place, adequately designed, and operating effectively. The review was conducted as part of our audit of the FDIC financial statements of 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, plans, 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 year 2015 and 2014 financial statements of the two funds administered by FDIC.

We evaluated and tested certain FDIC information systems controls, including the follow-up on the status of FDIC's corrective actions during calendar year 2015 to address open recommendations from our prior years' reports.

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, 2014 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 (NFE); 2) Communication, Capability, Challenge, and Control System (4C); 3) Portfolio Investment Accounting (PORTIA); 4) Assessment Information Management System (AIMS); 5) programs, data, and systems supporting the preparation of the estimates of losses and costs due to shared loss agreements; 6) and 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 as well as FDIC's policies and procedures, we evaluated controls by

- reviewing password settings to determine if password management was being enforced in accordance with agency policy;
- analyzing user system authorizations to determine whether users had more permissions than necessary to perform their assigned functions;
- observing methods for providing secure data transmissions to determine whether sensitive data were being encrypted;
- assessing configuration settings to evaluate settings used to audit security-relevant events; and
- inspecting vulnerability scans for in-scope systems to determine whether patches, service packs, and hot fixes 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

- examining an FDIC Office of Inspector General (OIG) report for information on FDIC's implementation of risk management policies;
- reviewing information security policies to determine whether they were adequately documented and implemented;
- examining an FDIC OIG report for information on specialized training;
- reviewing assessments of security controls to determine if they had been completed as scheduled;
- reviewing an FDIC OIG report for information on the corporation's information security continuous monitoring program;
- examining remedial action plans to determine whether FDIC had addressed identified vulnerabilities in a timely manner; and

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

-
- examining an FDIC OIG report for information on findings related to FDIC's remedial action process.

We performed our work in accordance with U.S. generally accepted government auditing standards. We believe that our audit work provided a reasonable basis for our conclusion in this report.

Appendix II: Comments from the Federal Deposit Insurance Corporation



Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Deputy to the Chairman and CFO

June 22, 2016

Mr. Gregory C. Wilshusen
Director, Information Security Issues
Dr. Nabajyoti Barkakati
Director, Center for Science, Technology, and Engineering
U.S. Government Accountability Office
Washington, D.C. 20548

Dear Mr. Wilshusen 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 Implemented Controls over Financial Systems, but Further Improvements Are Needed; GAO-16-605.

During the audit year, the FDIC management and staff worked to improve the information security program and controls and will continue to focus on this area in the coming 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.

We are pleased to have GAO acknowledge that, although the weaknesses identified warrant FDIC management's attention they do not individually or collectively amount to either a material weakness or a significant deficiency for financial reporting purposes. The GAO's report contains two recommendations to help the FDIC improve implementation of its information security program. Corrective actions will be completed during 2016 for one of the recommendations. Corrective action for the remaining one will involve a multi-year effort to ensure an effective solution. FDIC response details for the two recommendations are included in Attachment 1.

Once again, we thank you for your past contributions and your work on this year's audit. We appreciate the recognition in the report of some of the security improvements FDIC has made in the past year. 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 James H. Angel, Jr., Deputy Director, Corporate Management Control Branch, Division of Finance, at 703-562-6456.

Sincerely,

A handwritten signature in blue ink that reads "Steven O. App".

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

Attachment

**Appendix II: Comments from the Federal
Deposit Insurance Corporation**

Mr. G. Wilshusen and Dr. N. Barkakati

June 22, 2016

cc: James H. Angel, Jr.
Bret Edwards
Diane Ellis
Lawrence Gross, Jr.
Craig Jarvill
Arleas Upton Kea
Audit Committee

- 2 -

Attachment 1

FDIC RESPONSE DETAILS

Periodic Review Follow-up Action

Update access control procedures to require that authorizations for the removal or modification of access rights are documented and that approved changes are acted on in a timely manner.

Recommendation 1 – Concur; Expected Completion Date 10/15/2016

We recognize the need for improvements and will do so. We believe there were disparate causes for the issues identified, and our corrective actions are planned accordingly. The key changes that we will be making involve better resource management for one system and business owners reasserting ownership for two others where responsibility was shared with or delegated to other FDIC personnel. Procedures or similar documentation will be updated as appropriate in the course of making these changes. Our more detailed action plans have been provided to GAO in response to several recommendations from the related limited distribution report.

Audit and Monitoring

Develop and implement a policy that requires the monitoring of critical file changes for the platforms identified during the audit.

Recommendation 2 - Concur; Expected Completion Date 11/22/2016 (for interim milestone)

FDIC will develop a CIOO policy that will identify the scope of and responsibilities for monitoring critical files for server operating systems. The implementation of the policy is being addressed by FDIC in response to two recommendations from the related limited distribution report.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov

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

Staff Acknowledgments

In addition to the individuals named above, Gary Austin and Nick Marinos (Assistant Directors), Rosanna Guerrero (Analyst in Charge), Nancy Glover, Fatima Jahan, Franklin Jackson, Thomas J. Johnson, George Kovachick, Alan MacMullin, David Plocher, and Adam Vodraska made key contributions to this report.

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](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#).
Listen to our [Podcasts](#) and read [The Watchblog](#).
Visit GAO on the web at www.gao.gov.

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



Please Print on Recycled Paper.