



April 2015

INFORMATION SECURITY

FDIC Implemented Many Controls over Financial Systems, but Opportunities for Improvement Remain

Accessible Version

GAO Highlights

Highlights of [GAO-15-426](#), 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 the importance of FDIC's work, 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 audits of the 2014 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

GAO is making two recommendations to FDIC to improve its implementation of its information security program. FDIC concurred with GAO's recommendations. In a separate report with limited distribution, GAO is recommending that FDIC take five specific actions to address weaknesses in security controls.

View [GAO-15-426](#). 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.

April 2015

INFORMATION SECURITY

FDIC Implemented Many Controls over Financial Systems, but Opportunities for Improvement Remain

What GAO Found

The Federal Deposit Insurance Corporation (FDIC) has implemented numerous information security controls intended to protect its key financial systems; nevertheless, weaknesses remain that place the confidentiality, integrity, and availability of financial systems and information at risk. During 2014, the corporation implemented 27 of the 36 GAO recommendations pertaining to previously reported security weaknesses that were unaddressed as of December 31, 2013; actions to implement the remaining 9 recommendations were in progress. The table below details the status of these recommendations.

Status of Previously Reported Information Security Recommendations			
Year reported	Not implemented at the beginning of 2014	Implemented during 2014	Actions in progress
2010	1 ^a	1	0
2012	1 ^b	1	0
2013	9 ^c	6	3
2014	25	19	6
Total	36	27	9

Source: GAO analysis of FDIC data. | [GAO-15-426](#)

^aFDIC had previously implemented 32 of the 33 recommendations GAO originally reported in 2010.

^bFDIC had previously implemented 41 of the 42 recommendations GAO originally reported in 2012.

^cFDIC had previously implemented 21 of the 30 recommendations GAO originally reported in 2013.

Although FDIC developed and implemented elements of its information security program, shortcomings remain in key program activities. For example:

- FDIC had taken steps to improve its security policies and procedures, but important activities were not always required by its policies. For example, although FDIC had a policy on controlling physical access to its primary data center, the policy did not apply to all FDIC data centers.
- FDIC did not consistently remediate agency-identified weaknesses in a timely manner. However, to its credit, the corporation created a strategy outlining planned actions to address weaknesses in its remedial action processes.

Additionally, FDIC has designed and documented numerous information security controls intended to protect its key financial systems; nevertheless, controls were not always consistently implemented. For example, the corporation had not always (1) ensured that passwords for a financial application complied with FDIC policy for password length or (2) centrally collected audit logs on certain servers.

These weaknesses individually or collectively do not constitute either a material weakness or a significant deficiency for financial reporting purposes. Nonetheless, by mitigating known information security weaknesses and consistently applying information security controls, 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.

Contents

Letter	1
Background	2
FDIC Had Developed and Documented Many Controls to Secure Its Financial Information and Systems, but Improvements Are Still Needed	7
Conclusions	17
Recommendations for Executive Action	18
Agency Comments	18

Appendix I: Objective, Scope, and Methodology	20
Appendix II: Comments from the Federal Deposit Insurance Corporation	23
Appendix III: GAO Contacts and Staff Acknowledgments	24
GAO Contacts	24
Staff Acknowledgments	24

Abbreviations

DIF	Deposit Insurance Fund
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
FRF	Federal Savings and Loan Insurance Corporation Resolution Fund
IT	information technology
NIST	National Institute of Standards and Technology
POA&M	plan of action and milestones
SP	special publication
US-CERT	United States Computer Emergency Readiness Team

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.



Letter

U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

April 9, 2015

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, FDIC relies extensively on computerized systems. Because the corporation 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 FDIC 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 2014 financial statements of the Deposit Insurance Fund and the Federal Savings and Loan Insurance Corporation Resolution Fund, we assessed the effectiveness of FDIC's information security controls over key financial systems, data, and networks.¹ In our audit report, we concluded that FDIC maintained, in all material respects, effective internal control over financial reporting as of December 31, 2014, based on criteria established under the Federal Managers' Financial Integrity Act of 1982.²

In this report, we provide additional details on FDIC's information security controls over its computerized financial systems during 2014. 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. To do this, we examined FDIC information security policies, plans, and procedures; tested controls over its key

¹GAO, *Financial Audit: Federal Deposit Insurance Corporation Funds' 2014 and 2013 Financial Statements*, [GAO-15-289](#) (Washington, D.C.: Feb. 12, 2015).

²31 U.S.C. § 3512(c) and (d).

financial applications; reviewed our prior reports to identify previously reported weaknesses and assess the effectiveness of corrective actions taken; and interviewed agency officials. This work was performed to support our opinion on FDIC's internal control over financial reporting as of December 31, 2014.

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. See appendix I for more details on our objective, scope, and methodology.

Background

Information security is a critical consideration for any agency that depends on information systems and computer networks to carry out its mission and is especially important for a government corporation such as FDIC, which has responsibilities to oversee the financial institutions that are entrusted with safeguarding the public's money. While the use of interconnected electronic information systems allows the corporation to accomplish its mission more quickly and effectively, this also exposes FDIC's information to threats from sources internal and external to the agency. Internal threats include errors, as well as fraudulent or malevolent acts by employees or contractors working within the agency. External threats include the ever-growing number of cyber-based attacks that can come from a variety of sources such as hackers, criminals, foreign nations, terrorists, and other adversarial groups.

Potential cyber attackers have a variety of techniques at their disposal, which can vastly enhance the reach and impact of their actions. For example, cyber attackers do not need to be physically close to their targets, their attacks can easily cross state and national borders, and they can preserve their anonymity. Additionally, advanced persistent threats—where an adversary that possesses sophisticated levels of expertise and significant resources can attack using physical and cyber methods to achieve its objectives³—pose increasing risks. Further, the

³These objectives typically include establishing/extending footholds within the information technology infrastructure of the targeted agency for purposes of exfiltrating information; undermining or impeding critical aspects of a mission, program, or agency; or positioning itself to carry out these objectives in the future. An advanced persistent threat (1) pursues its objectives repeatedly over an extended period of time, (2) adapts to defenders' efforts to resist it, and (3) maintains the level of interaction needed to achieve its objectives.

interconnectivity among information systems presents increasing opportunities for such attacks. Indeed, reports of security incidents from federal agencies are on the rise. Specifically, the number of incidents reported by federal agencies to the United States Computer Emergency Readiness Team⁴ (US-CERT) has increased dramatically in recent years: from 5,503 incidents reported in fiscal year 2006 to 67,168 incidents in fiscal year 2014.

Compounding the growing number and types of threats are the deficiencies in security controls on the information systems at federal agencies, which have resulted in vulnerabilities in both financial and nonfinancial systems and information. These deficiencies continue to place assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, and critical operations at risk of disruption. Accordingly, we have designated information security as a government-wide high-risk area since 1997, a designation that remains in force today.⁵

Federal law and guidance specify requirements for protecting federal information and information systems. The Federal Information Security Management Act of 2002 (FISMA)⁶ provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. To accomplish this, FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide information security for the information and systems that support its operations and assets, using a risk-based approach to information security management. Such a program includes assessing risk; developing and implementing cost-effective security plans, policies, and

⁴The Department of Homeland Security's federal information security incident center is hosted by US-CERT. When incidents occur, agencies are to notify the center.

⁵GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997) and *High Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: February 2015).

⁶FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As our review was finishing, the Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (Dec. 18, 2014), was enacted. However, the new law, which partially supersedes FISMA, incorporates and continues the requirements from FISMA that we relied upon in our report. Accordingly, no changes to our findings were necessary.

procedures; providing specialized training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; and ensuring continuity of operations.

FISMA also assigned to the National Institute of Standards and Technology (NIST) the responsibility for developing standards and guidelines that include minimum information security requirements. To this end, NIST has issued several publications to provide guidance for agencies in implementing an information security program. For example, NIST Federal Information Processing Standard (FIPS) 199⁷ provides requirements on how agencies should categorize their information and information system(s) and NIST special publication (SP) 800-53⁸ provides guidance to agencies on the selection and implementation of information security and privacy controls for systems.

FDIC Is a Key Protector of Bank and Thrift Deposits

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. FDIC is an independent agency of the federal government, which Congress created in 1933⁹ in response to the thousands of bank failures that had occurred throughout the late 1920s and early 1930s.¹⁰ FDIC insures deposits in banks and thrift institutions for at least \$250,000; identifies, monitors, and addresses risks to the deposit insurance funds; and limits the effect on the economy and the financial system when a bank or thrift institution fails.

⁷NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004).

⁸NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

⁹Federal Deposit Insurance Corporation Act, June 16, 1933, Ch. 89, § 8.

¹⁰FDIC receives no congressional 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.

FDIC administers two funds in carrying out its mission:

- The Deposit Insurance Fund (DIF) has the primary purposes of (1) insuring the deposits and protecting the depositors of banks and savings associations (insured depository institutions) and (2) resolving failed insured depository institutions in a manner that will result in the least possible cost to the fund. In cooperation with other federal and state agencies, FDIC promotes the safety and soundness of insured depository institutions by identifying, monitoring, and addressing risks to the DIF.
- The Federal Savings and Loan Insurance Corporation Resolution Fund (FRF) is responsible for the sale of the remaining assets and the satisfaction of the liabilities associated with the former Federal Savings and Loan Insurance Corporation and the former Resolution Trust Corporation.

FDIC maintains the DIF and the FRF separately to support their respective functions.¹¹

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 security defense.

To support its financial management functions, FDIC uses

- a corporate-wide system that functions as a unified set of financial and payroll systems that are managed and operated in an integrated fashion;

¹¹A third fund to be managed by FDIC, the Orderly Liquidation Fund, established by section 210 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376, 1506 (July 21, 2010), is unfunded and conducted no transactions during the fiscal years covered by this audit.

- a system to calculate and collect FDIC deposit insurance premiums and Financing Corporation¹² bond principal and interest amounts from insured financial institutions;
- a web-based application that provides full functionality to support franchise marketing, 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;
- 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.

Under FISMA, the Chairman of FDIC is responsible for, among other things,

- 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;
- ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control; and
- delegating to the corporation's Chief Information Officer the authority to ensure compliance with the requirements imposed on the agency under FISMA.

¹²The Financing Corporation, established by the Competitive Equality Banking Act of 1987, is a mixed-ownership government corporation whose primary purpose is 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 non-callable bonds with a principal amount of approximately \$8.1 billion, mature in 2017 through 2019.

The Chief Information Officer 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 Chief Information Officer 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 Chief Information Officer and serves as the Chief Information Officer's designated representative. The 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.

FDIC Had Developed and Documented Many Controls to Secure Its Financial Information and Systems, but Improvements Are Still Needed

Although FDIC developed and implemented elements of its information security program, the corporation did not always implement key program activities. Additionally, FDIC has designed and documented numerous information security controls intended to protect its key financial systems; however, shortcomings existed in the implementation of other information security controls. 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.

FDIC Continues to Make Progress in Implementing Its Information Security Program

An entity-wide 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

- plans for providing adequate information security for networks, facilities, and systems;
- security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;
- policies and procedures that (1) are based on risk assessments, (2) cost effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in its information security policies, procedures, or practices; and
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems.

FDIC Developed and Documented Elements of Its Corporate Information Security Program

FDIC made improvements in developing and documenting many elements of its corporate information security program. For example:

- During 2014, FDIC completed actions to address two weaknesses we previously reported related to system security planning. Specifically, the corporation had ensured that the system security plans for three applications thoroughly described each control and included all required information, and ensured that descriptions of common controls were adequately documented.
- During 2014, FDIC addressed our prior recommendation to ensure that those with administrative-level access have completed the requisite rules of behavior training upon receiving access and each year after that.
- FDIC had taken steps to document, implement, and improve policies for information security. Specifically, in June 2014, the corporation formalized a new policy on security patch management. The policy defines risk categories for patches, time frames for applying patches based on the risk categories and platform-specific requirements, and roles and responsibilities for patch management. Additionally, the FDIC Office of the Inspector General reported in November 2014 that

FDIC had drafted a new information technology (IT) security risk management program policy that was designed to align with NIST and Office of Management and Budget guidance and reflect the corporation's information security risk management program and governance structure.

- FDIC addressed many weaknesses that we previously identified in its information systems supporting financial processing. Specifically, during 2014, FDIC implemented 27 of the 36 recommendations pertaining to unaddressed security weaknesses that we previously reported, and actions to correct or mitigate the remaining 9 weaknesses were in progress.

Information Security Program Continues to Present Opportunities for Improvement

Although FDIC continues to improve its implementation of its corporate information security program, shortcomings existed in other information security program elements. Specifically:

- FDIC's information security policies and procedures did not always include important requirements. NIST special publication (SP) 800-53 Revision 4 recommends that agencies regularly review individuals' physical access to facilities and remove that access when it is no longer required. However, although FDIC had a policy on controlling physical access to its primary data center, the corporation did not recertify access to its backup data center because the policy did not apply to all FDIC data centers. Additionally, although FDIC policy states that access to IT resources is to be provided only after proper authorization has been provided, the corporation did not document that it had verified access to a system supporting the marketing of failed banks' assets because its existing procedures did not require the access verifications to be documented. As a result, there is an increased risk that individuals who no longer need access to information systems could accidentally or intentionally damage critical resources.
- Improvements are needed in the corporation's continuous monitoring program. To its credit, the corporation conducted control assessments of the major applications and general support systems we reviewed and addressed a weakness we previously identified by assessing security controls for two systems in accordance with its assessment schedule. In addition, the FDIC Office of Inspector General reported in November 2014 that FDIC had performed a number of continuous monitoring activities, developed an assessment methodology that defined a risk-focused approach for performing continuous monitoring on information systems, and reported various continuous monitoring metrics to senior managers. However, the office reported that the

corporation had not yet developed a written, corporate-wide information security continuous monitoring strategy that included key elements from NIST guidance for continuous monitoring. The office recommended that FDIC develop and approve a written continuous monitoring strategy consistent with Office of Management and Budget and NIST guidance. Until this recommendation is addressed, FDIC will have limited assurance that the controls are operating effectively to protect its financial systems and information.

- Improvements are needed in the corporation's remedial action processes. Specifically, at the time of our review, 25 of the 285 remedial action plans applicable to agency information systems in our audit scope were past their expected closure dates by between about 2 weeks and 10 months, including 4 high-risk items. In addition, the FDIC Office of Inspector General reported in November 2014 that, as of July 2014, the corporation's remedial action management system contained a large number of high- and moderate-risk security vulnerabilities, many of which had planned corrective actions that were significantly past their scheduled completion dates. The Office also reported that FDIC has taken steps to improve its remedial action processes by creating a strategy outlining planned actions to address weaknesses in the corporation's plan of action and milestones processes. Nevertheless, until FDIC fully addresses shortcomings in its remedial action processes, the corporation's financial information and systems will remain at increased and unnecessary risk. Because the FDIC Office of Inspector General has already made recommendations to address shortcomings in FDIC's remedial action processes, we are not making additional recommendations in this area.

FDIC Implemented Many Controls, but Shortcomings Still Warrant Management Attention

An agency can protect the resources that support its critical operations and assets from unauthorized access, disclosure, modification, or loss by designing and implementing controls for segregating incompatible duties, identifying and authenticating users, restricting user access to only what has been authorized, 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.

Controls for Segregation of Incompatible Duties Improved

To reduce the risk of error or fraud, duties and responsibilities for authorizing, processing, recording, and reviewing transactions should be separated to ensure that one user does not control all of the critical stages of a process. NIST SP 800-53 Revision 4 states that, to prevent malevolent activity without collusion, organizations should separate the duties of users as necessary and implement separation of duties through defined information system access authorizations. Additionally, consistent with NIST guidance, FDIC policy on access control for IT resources states that, where required, access controls shall be used to enforce the principle of separation of duties to restrict the level of access and ability provided to any single user.

FDIC improved its implementation of segregation of duties controls by implementing four recommendations we had previously made pertaining to segregation of duties. For example, FDIC identified and documented incompatible roles and established processes and procedures to enforce segregation of duties for several applications and systems supporting financial processing. Additionally, the corporation had restricted users with access to source code for a financial system from having access to that system's production environment. As a result, FDIC has reduced its risk that users could conduct fraudulent activity by bypassing intended controls.

Improvements Made in Controls for Identifying and Authenticating Users, but Password Controls Were Not Always Implemented

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 ID combination. Consistent with NIST SP 800-53 Revision 4, FDIC policy establishes minimum password length and complexity requirements.

During 2014, FDIC improved controls for identifying and authenticating the identity of users by implementing two recommendations that we had previously made and that were still unresolved as of December 31, 2013. For example, FDIC had disallowed the use of default credentials for access to an application supporting FDIC's process for managing cash and investment transactions and had provided password lifetime and complexity controls to user accounts for a database that supported financial processing.

However, FDIC did not fully implement password controls on the application supporting its process for managing cash and investment transactions in accordance with its policy. Specifically, passwords for the

Controls for Restricting Access to Only What Users Needed Were Largely Effective, but Shortcomings Remain

application did not comply with the minimum length standards established by FDIC's password policy. As a result, there is an increased likelihood 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 access for users (or processes acting on behalf of users) which are 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. NIST also 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. Consistent with NIST guidance, FDIC policy also states that access to IT resources shall be terminated immediately 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 2014, FDIC improved controls for authorizing users' access by implementing 11 of 12 recommendations we had previously made pertaining to authorization controls and that were still unresolved as of December 31, 2013. For example, FDIC had

- ensured that accounts belonging to users who had not accessed certain applications and systems in a predefined period of time were disabled,
- discontinued the use of shared user IDs for several applications and databases supporting financial processing,

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

-
- removed certain users' excessive access to an application supporting FDIC's process for estimating potential losses from litigation, and
 - restricted access to the network shared folder where annual financial statements and footnotes were maintained.

Although improvements were made, FDIC did not always implement sufficient authorization controls. For example, as discussed earlier, the corporation did not recertify the need for data center access on a periodic basis to ensure that individuals' access remained appropriate, and did not always recertify account access to an application used by FDIC to store loan data for failing financial institutions. Additionally, the corporation had not yet completed actions to implement our prior-year recommendation to ensure that accounts for users who have access to the network and who have been separated from employment are removed immediately upon separation.

Although these weaknesses did not materially impact FDIC's financial statements, they nevertheless increase the risk that individuals may have greater access to data centers or to financial information and systems than they need to fulfill their responsibilities, or that user accounts for departed individuals could be used to gain unauthorized access to systems that process sensitive financial information.

FDIC Used Strong Encryption for Two Systems, but Did Not Always Sufficiently Encrypt Sensitive Connections

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 Special Publication 800-53 Revision 4 recommends that organizations employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission, encrypt passwords while being stored and transmitted, and establish a trusted communications path between users and security functions of information systems. The

NIST standard for an encryption algorithm is Federal Information Processing Standard (FIPS) 140-2.¹⁴

FDIC improved its encryption controls by implementing our prior-year recommendation to use FIPS 140-2-compliant encryption for protection of authentication and session data for two systems supporting financial processing. However, FDIC had not completed actions to implement our prior recommendation to use FIPS-compliant encryption for all mainframe connections. As a result, sensitive data transmitted over these connections could be exposed to potential compromise.

Audit and Monitoring Controls Improved, but Opportunities for Improvement Remain

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. Audit and monitoring technologies include network and host-based intrusion detection systems, audit logging, security event correlation tools, and computer forensics. 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 officials. Additionally, NIST states that audit records should contain information on individual audit events, including their type, source, and outcome, as well as the date and time that they occurred and any individuals or subjects associated with the events, among other things.

FDIC improved its audit and monitoring controls by implementing three of six recommendations pertaining to audit and monitoring that we had previously identified and that were still unresolved as of December 31, 2013. For example, the corporation had ensured that log history for privileged accounts on key servers supporting financial processing were sufficient to aid incident response and forensic investigations.

¹⁴NIST, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Gaithersburg, Md.: May 2001).

However, FDIC had not yet completed actions to address three weaknesses related to auditing and monitoring controls we previously identified. For example, the corporation had not yet ensured that, for certain systems, sensitive and high-risk events are consistently logged. In addition, FDIC did not always effectively monitor server security logs. Specifically, three servers supporting financial processing did not send log output to the corporation's centralized audit logging system.

While the three outstanding recommendations and the additional weakness identified this year 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, or that sufficient data would not be available, hindering efforts to investigate potential security incidents after the fact.

Configuration Management
Shortcomings Increase
Risk to Financial Systems
and Information

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. Patch management, a component of configuration management, is important for mitigating the risks associated with software vulnerabilities. When a software vulnerability is discovered, the software vendor may develop and distribute a patch or work-around to mitigate the vulnerability. Without the patch, an attacker can exploit the vulnerability to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other systems.

NIST SP 800-53 Revision 4 states that organizations should establish a baseline configuration for the information system and its constituent components. Additionally, FDIC policy states that FDIC must establish and document mandatory configuration settings for IT products employed within the information system using information-system-defined security configuration checklists. Further, NIST SP 800-128¹⁵ states that patch

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

management procedures should define how the organization's patch management process is integrated into configuration management processes, how patches are prioritized and approved through the configuration change control process, and how patches are tested for their impact on existing secure configurations.

Although improvements were made, shortcomings remain in FDIC's implementation of configuration management controls. FDIC had made progress toward addressing our prior recommendation to establish baseline configurations for all FDIC information systems by establishing agency-wide configuration settings for three platforms. According to officials, FDIC plans to establish baselines for the majority of its platforms by the end of 2015. In addition, 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 completed actions to address our prior recommendation to apply patches to remediate known vulnerabilities in third-party software.

These issues did not materially affect the corporation's financial statements. Nevertheless, until our previously identified weaknesses are addressed, FDIC faces increased 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 Had Not Yet Corrected
Employee Background
Investigation Issue

Policies related to hiring and management of personnel are important considerations in securing information systems. If personnel policies are not adequate, an entity runs the risk of (1) hiring unqualified or untrustworthy individuals; (2) providing terminated employees opportunities to sabotage or otherwise impair entity operations or assets; (3) failing to detect continuing unauthorized employee actions; (4) lowering employee morale, which may in turn diminish employee compliance with controls; and (5) allowing staff expertise to decline. Personnel procedures should include contacting references, 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. FDIC policy states that personnel in moderate- and low-risk positions should be subject to a background reinvestigation every 5 and 7 years, respectively.

In 2014, we reported that background reinvestigations were not being performed in accordance with FDIC policy; specifically, background reinvestigations had not been performed prior to Fall 2013 for users with a security rating less than high risk. During our current review, FDIC officials stated that their planned efforts to address this weakness will not be completed until April 2016. Until this weakness is fully addressed, FDIC will continue to face elevated risk that it will not identify malicious users of financial applications who would commit or attempt to commit fraud.

Conclusions

FDIC had developed, documented, and implemented many elements of its corporate information security program. For example, the corporation had formalized a new policy for information security patch management and had ensured that administrators completed required training. In addition, 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 segregating incompatible duties, identifying and authenticating users, restricting user access to only what has been authorized, encrypting of sensitive data, and auditing and monitoring systems for potentially malicious activity, by addressing many of the weaknesses that we previously reported.

However, management attention is still needed to address shortcomings in the corporation's information security program. For example, shortcomings in certain security policies and procedures led to weaknesses in conducting and documenting reviews of user access. Additionally, further actions are needed to address weaknesses in identification and authentication, authorization, and audit and monitoring controls. Given the important role that information systems play in FDIC's internal controls over financial reporting, it is vitally important that FDIC address the remaining 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. Although we do not consider these weaknesses individually or collectively to be either a material weakness or a significant deficiency for financial reporting purposes, we are nevertheless making five recommendations in a separate product with limited distribution for FDIC to address new weaknesses we identified in this review. Until FDIC takes further steps to mitigate these weaknesses, the corporation's sensitive financial information and resources will remain unnecessarily exposed to increased risk of inadvertent or deliberate misuse, improper modification, unauthorized disclosure, or destruction.

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 two actions:

- Ensure that physical access policies require periodic review of access to all FDIC data centers.
- Update existing procedures to require that access verifications to the system supporting the marketing of failed banks' assets be documented.

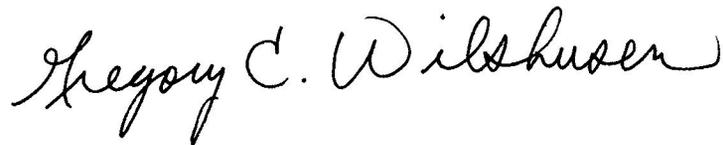
Additionally, in a separate report with limited distribution, we are making five recommendations consisting of actions to implement and correct specific information security weaknesses related to identification and authentication, authorization, and audit and monitoring.

Agency Comments

In providing written comments (reprinted in app. II) on a draft of this report, FDIC stated that corrective actions for the two new recommendations have already been or will be completed during 2015. FDIC also provided an attachment detailing its actions to implement our recommendations as well as technical comments that we addressed in our report as appropriate.

We are sending copies of this report to interested congressional parties. In addition, this 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 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. 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 and plans; controls over key financial systems; and interviews with agency officials 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 2014 and 2013 financial statements of the two funds administered by FDIC.

GAO used an independent public accounting firm, under contract, to evaluate and test certain FDIC information systems controls, including the follow-up on the status of FDIC's corrective actions during calendar year 2014 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 FDIC's actions to mitigate previously reported weaknesses that remained open as of December 31, 2013, 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. 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

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

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

- examining access responsibilities to determine whether incompatible functions were segregated among different individuals;
- reviewed 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 Management Act of 2002, which establishes elements for an agency-wide information security program, we evaluated FDIC's implementation of its security program by

- analyzing security plans for key financial systems to determine whether management, operational, and technical controls had been documented and whether security plans had been updated regularly in accordance with NIST requirements;
- reviewing training records for administrators to determine if they had received training appropriate to their responsibilities;
- reviewing information security policies to determine whether they were adequately documented and implemented;
- examining an FDIC Office of Inspector General report for information on FDIC's implementation of risk management policies;
- reviewing ongoing assessments of security controls to determine if they had been completed as scheduled;

- reviewing an FDIC Office of Inspector General report for information on the corporation's information security continuous monitoring program;
- examining remedial action plans to determine whether FDIC addressed identified vulnerabilities in a timely manner; and
- examining an FDIC Office of Inspector General report for information on findings related to FDIC's remedial action process.

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 and examined FDIC's corrective action plans to determine which weaknesses FDIC had reported as being corrected. For those instances where FDIC reported it had completed corrective actions, we assessed the effectiveness of those actions.

We performed our work from June 2014 to April 2015 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

March 19, 2015

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 Many Controls over Financial Systems, but Opportunities for Improvement Remain: GAO-15-426.

The GAO's report contains two recommendations to help the FDIC improve implementation of its information security program. Corrective actions have already been or will be completed during 2015 for the two recommendations. 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 look forward to continuing our positive working relationship during the 2015 audit and beyond. 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

Attachments

cc: James H. Angel, Jr.,
Bret Edwards
Craig Jarvill
Arleas Upton Kea
Barry C. West
Audit Committee

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), William Cook, Thomas J. Johnson, George Kovachick, and Lee McCracken 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](#).
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