

November 2010

**INFORMATION
SECURITY**

**Federal Deposit
Insurance Corporation
Needs to Mitigate
Control Weaknesses**



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-11-29](#), a report to the Chairman, Federal Deposit Insurance Corporation

Why GAO Did This Study

The Federal Deposit Insurance Corporation (FDIC) has a demanding responsibility enforcing banking laws, regulating financial institutions, and protecting depositors. Because of the importance of its work, the corporation must employ strong information security controls to ensure that its information systems are adequately protected from inadvertent misuse, fraud, and improper disclosure.

As part of its audit of the 2009 financial statements of the Deposit Insurance Fund and the Federal Savings & Loan Insurance Corporation Resolution Fund administered by FDIC, GAO assessed (1) the effectiveness of FDIC's controls in protecting the confidentiality, integrity, and availability of its financial systems and information and (2) the progress FDIC has made in mitigating previously reported information security weaknesses. To perform the audit, GAO examined security policies, procedures, reports, and other documents; tested controls over key financial applications; and interviewed key FDIC personnel.

What GAO Recommends

GAO is recommending that FDIC improve key information activities to enhance the corporation's information security program. FDIC generally agreed with GAO's recommendations and stated that it plans to address the identified weaknesses.

View [GAO-11-29](#) or key components. 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

November 2010

INFORMATION SECURITY

Federal Deposit Insurance Corporation Needs to Mitigate Control Weaknesses

What GAO Found

FDIC did not sufficiently implement access and other controls intended to protect the confidentiality, integrity, and availability of its financial systems and information. For example, it did not always

- sufficiently restrict user access to systems,
- ensure strong system boundaries,
- consistently enforce strong controls for identifying and authenticating users,
- encrypt sensitive information, or
- audit and monitor security-relevant events.

In addition, FDIC did not have policies, procedures, and controls in place to ensure the appropriate segregation of incompatible duties, adequately manage the configuration of its financial information systems, and update contingency plans. A key reason for these weaknesses is that FDIC did not always fully implement key information security program activities such as effectively developing, documenting, and implementing security policies, and implementing an effective continuous monitoring program. Until these weaknesses and program deficiencies are corrected, the corporation will not have sufficient assurance that its financial information and assets are adequately safeguarded from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

Despite the newly identified weaknesses, FDIC has mitigated each of the information security weaknesses previously reported by GAO. To its credit, the corporation has made improvements to its configuration management controls and aspects of its security management. For example, it maintained a full and complete requirements baseline for two systems and included key information in a remedial action plan.

Nevertheless, GAO concluded that weaknesses in information security controls constituted a significant deficiency in internal controls over the information systems and data used for financial reporting. Until FDIC corrects the security weaknesses identified during this year's audit, it will face an elevated risk of the misuse of federal assets, unauthorized modification or destruction of financial information, inappropriate disclosure of other sensitive information, and disruption of critical operations.

Contents

Letter		1
	Background	2
	Information Security Weaknesses Place Financial and Other Sensitive Information at Risk	6
	FDIC Has Mitigated Previously Reported Weaknesses	16
	Conclusions	17
	Recommendations for Executive Action	17
	Agency Comments	18
Appendix I	Objectives, Scope, and Methodology	19
Appendix II	Comments from the Federal Deposit Insurance Corporation	22
Appendix III	GAO Contacts and Staff Acknowledgments	24

Abbreviations

DHS	Department of Homeland Security
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Act
ID	identification
IP	Internet Protocol
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
SNMP	Simple Network Management Protocol
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.



G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

November 30, 2010

The Honorable Sheila C. Bair
Chairman
Federal Deposit Insurance Corporation

Dear Madame Chairman:

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 FDIC 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 adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.¹

As part of our audit of FDIC's calendar year 2009 financial statements of the Deposit Insurance Fund and the Federal Savings & Loan Insurance Corporation Resolution Fund, we assessed the effectiveness of FDIC's information security controls over key financial systems, data, and networks.² In that report, we concluded that weaknesses in information security controls collectively constituted a significant deficiency in

¹Information system general controls affect the overall effectiveness and security of computer operations and are not unique to specific computer applications. These controls include security management, configuration management, operating procedures, software security features, and physical protections designed to ensure that access to data is appropriately restricted, that only authorized changes to computer programs are made, that incompatible computer-related duties are segregated, and that backup and recovery plans are adequate to ensure the continuity of operations.

²GAO, *Financial Audit: Federal Deposit Insurance Corporation Funds' 2009 and 2008 Financial Statements*, GAO-10-705 (Washington, D.C.: June 25, 2010).

internal controls over the information systems and data used for financial reporting.³

In this report, we provide additional details on FDIC's information security controls during calendar year 2009. Our specific objectives were to assess (1) the effectiveness of its controls for ensuring the confidentiality, integrity, and availability of its financial information systems and information and (2) the status of FDIC's actions to correct or mitigate previously reported information security weaknesses. We conducted this performance audit at FDIC facilities in Arlington, Virginia; Washington, D.C.; and Dallas, Texas, from December 2009 to November 2010 in accordance with generally accepted government auditing standards.⁴ 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 our audit provides a reasonable basis for our findings and conclusions. See appendix I for additional details on our objectives, scope, and methodology.

Background

Information security is a critical consideration for any organization 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 oversees the financial institutions that are entrusted with safeguarding the public's money. While the use of interconnected electronic information systems allows FDIC to accomplish its mission more quickly and effectively, their use also exposes FDIC's information to the various internal and external threats that come with the use of such systems.

Cyber-based threats to information systems and cyber-related critical infrastructure are evolving and growing and can affect FDIC information

³A significant deficiency is a control deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

⁴We performed data collection, analysis, and assessment procedures in support of the financial audit during the December 2009 to June 2010 time frame. We performed supplemental audit procedures to prepare this report from June 2010 to November 2010.

systems and computer networks. Threats that could adversely affect the systems and information relevant to FDIC's operations associated with financial management and reporting can come from sources internal and external to the organization. Internal threats include mistakes by individuals, and fraudulent or malevolent acts by insiders. External threats include the ever-growing number of cyber-based attacks that can come from a variety of sources such as hackers, criminals, and foreign nations.

These potential 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 cyber attackers can readily preserve their anonymity. Further, the interconnectivity among information systems presents increasing opportunities for such attacks. Indeed, reports of security incidents from federal agencies are on the rise, increasing by more than 400 percent from fiscal year 2006 to fiscal year 2009. Specifically, the number of incidents reported by federal agencies to the United States Computer Emergency Readiness Team (US-CERT) has increased dramatically over the past 4 years: from 5,503 incidents reported in fiscal year 2006 to about 30,000 incidents in fiscal year 2009.⁵

Compounding the growing number and kinds of threats are the significant 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 governmentwide high-risk area since 1997, a designation that remains in force today.⁶ Recognizing the importance of securing federal agencies' information systems, Congress enacted the Federal Information Security Management Act (FISMA) in December 2002 to strengthen the security of

⁵The Department of Homeland Security's (DHS) federal information security incident center is hosted by US-CERT. When incidents occur, agencies are to notify the center.

⁶GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997), and *High-Risk Series: An Update*, [GAO-09-271](#) (Washington, D.C.: January 2009).

information and systems within federal agencies.⁷ FISMA requires each agency to develop, document, and implement an agencywide information security program to provide information security for the information and systems that support the operations and assets of the entities, using a risk-based approach to information security management.

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. Congress created FDIC in 1933⁸ in response to the thousands of bank failures that occurred in the 1920s and early 1930s.⁹ 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.¹⁰ The act also designated FDIC as the administrator of the Federal Savings & Loan Insurance Corporation Resolution Fund, which was created to complete the affairs of the former Federal Savings & Loan Insurance Corporation and liquidate the assets and liabilities transferred from the former Resolution Trust Corporation. The Bank Insurance Fund and the Savings Association Insurance Fund merged into the Deposit Insurance Fund on February 8, 2006, as a result of the passage of the Federal Deposit Insurance Reform Act of 2005.¹¹

⁷FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

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

⁹FDIC is an independent agency of the federal government and receives no direct 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.

¹⁰Pub. L. No. 101-73, § 211, 103 Stat. 183, 218-22 (Aug. 9, 1989).

¹¹Pub. L. No. 109-171, Title II, Subtitle B, § 2102 (Feb. 8, 2006).

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. Its local and wide area networks interconnect these systems. To support its financial management functions, the corporation relies on many systems, including a corporatewide system that functions as a unified set of financial and payroll systems that are managed together and operated in an integrated fashion, a system to calculate and collect FDIC deposit insurance premiums and Financing Corporation bond principal and interest amounts from insured financial institutions;¹² a Web-based application that provides full functionality to support franchise marketing, asset marketing, and asset management; 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. FDIC financial systems process and track financial transactions such as disbursements made to support operations. FDIC protects its computerized systems using a layered approach to security defense.

Under FISMA, 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 entity's information systems and information; (2) ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control; and (3) delegating to the corporation's Chief Information Officer the authority to ensure compliance with the requirements imposed on the agency under FISMA.

The Chief Information Officer is responsible for developing and maintaining a corporatewide 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

¹²The 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 & 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.

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 the overall support of certification and accreditation activities.¹³ According to FDIC policy, the Chief Information Security Officer is responsible for the development, coordination, and implementation of FDIC's security policy and the coordination of information security and privacy efforts across the corporation. The Chief Information Security Officer coordinates the process of building a corporatewide security strategy and vision to include the creation and maintenance of FDIC's information security policy, security risk assessment efforts, information technology risk assessments, disaster recovery, security monitoring, security awareness and training program, and security protection architecture.

Information Security Weaknesses Place Financial and Other Sensitive Information at Risk

FDIC did not sufficiently implement access and other controls intended to protect the confidentiality, integrity, and availability of its financial systems and information and other sensitive information. A key reason for these weaknesses is that FDIC did not always fully implement key information security program activities such as effectively developing and implementing security policies, and implementing an effective continuous monitoring program. These control deficiencies, which collectively constituted a significant deficiency for calendar year 2009, reduced FDIC's ability to ensure that authorized users had only the access needed to perform their assigned duties, and that its systems were sufficiently protected from unauthorized access. As a result, increased risk exists that financial information and other sensitive information could be disclosed or modified without authorization.

¹³The Office of Management and Budget (OMB) requires that a management official formally authorize (or accredit) an information system to process information and accept the risk associated with its operation based on a formal evaluation (or certification) of the system's security controls. For annual reporting, OMB requires agencies to report the number of systems, including impact levels, authorized for processing after completing certification and accreditation.

Access Controls to Information Resources Were Not Sufficient

A basic management objective for any organization is to protect the resources that support its critical operations and assets from unauthorized access. Organizations accomplish this by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computer resources (e.g., data, programs, equipment, and facilities), thereby protecting them from unauthorized disclosure, modification, and loss. Specific access controls include authorization restrictions, system boundary protections, identification and authentication of users, cryptography, and audit and monitoring procedures. Without adequate access controls, unauthorized individuals, including intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users can intentionally or unintentionally modify or delete data or execute changes that are outside of their authority.

User Access Was Not Sufficiently Restricted

Authorization is the process of granting or denying access rights and privileges to a protected resource, such as a network, system, application, function, or file. A key component of granting or denying access rights is the concept of “least privilege,” which refers to granting users only the access rights and permissions that they need to perform their official duties. To restrict legitimate users’ access to only those programs and files that they need in order to do their work, organizations establish user access rights: allowable actions that can be assigned to users or to groups of users. File and directory permissions are rules that are associated with a particular file or directory, regulating which users can access it—and the extent of their access rights. To avoid unintentionally giving a user unnecessary access to sensitive files and directories, an organization should give careful consideration to its assignment of rights and permissions. In addition, National Institute of Standards and Technology (NIST) guidance states that an organization should enforce approved authorizations for logical access to its information systems with access mechanisms such as access control lists within the network system.¹⁴ Furthermore, NIST guidance states that access should be allowed only for authorized users and only for the tasks necessary to accomplish their work in accordance with the organization’s missions and business functions.

¹⁴Logical access requires users to authenticate themselves (through the use of secret passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they can execute.

FDIC did not always sufficiently restrict system access and privileges to only those users who needed access to perform their assigned duties. For example, FDIC did not always

- configure access control lists on all its network devices to limit or restrict network traffic,
- configure access control lists on servers dedicated to network management to restrict access to only those users who require it,
- ensure access to sensitive files of critical network devices was adequately controlled,
- control access to a database supporting an accounting application used to process receivership asset financial activity, and
- limit user access rights to only those roles necessary to perform their duties.

As a result, increased risk exists that a user could gain inappropriate access to computer resources, circumvent security controls, and deliberately or inadvertently read, modify, or delete financial information and other sensitive information.

System Boundary Protections Were Not Adequately Enforced

Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from network-connected devices. Unnecessary connectivity to an organization's network increases not only the number of access paths that must be managed and the complexity of the task, but also the risks of unauthorized access. National Security Agency (NSA) guidelines state that, to reduce the probability of a successful network penetration, the data and telephony networks must be logically separated.

FDIC did not control access to its data network by separating or partitioning the data network from the voice network. Physical convergence of voice and data networks is an advantage of Internet Protocol (IP) telephony systems; however, placing both systems on the same network means both are now susceptible to the same attacks and the same attackers. As a result, increased risk exists that unauthorized or malicious users could gain access to the data network and inadvertently read, modify, or delete financial information and other sensitive information.

Identification and Authentication User Controls Were Not Consistently Enforced

A computer system must be able to identify and authenticate the identity of a user so that activities on the system can be linked to that specific individual and to protect its systems from inadvertent or malicious access. When an organization assigns unique user accounts to specific users, the system is able to distinguish one user from another—a process called identification. This allows the system to distinguish and track one user from another. The system must also establish the validity of the user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. The NSA security guidelines state that standard or default community strings should not be used.¹⁵ In addition, NIST guidance states that an organization should manage information system authenticators by changing the default content of authenticators (e.g., passwords) when installing an information system. Furthermore, FDIC policy states that passwords should be changed after 90 days.

FDIC did not consistently enforce identification and authentication controls for its users and systems. Specifically,

- FDIC had not securely configured the Simple Network Management Protocol (SNMP) community strings.¹⁶ Also, FDIC had not recently changed the SNMP read-write community string for administering routers and switches.
- An FDIC network software package was operating with a default vendor-supplied identification (ID) and password.
- Several service and administrator user accounts on UNIX servers were not required to change their passwords in accordance with FDIC policy or were set to never expire.

As a result of these weaknesses, increased risk exists that a user would not be uniquely identified before accessing the FDIC network, leaving

¹⁵The community string (also known as the community name) provides a weak authentication mechanism to the Simple Network Management Protocol (SNMP). Agents can be configured to allow read-only, read-write, or no access to their parameters based on the community string in a request. Community strings are passed in clear text in SNMP messages, so they can be easily sniffed and are therefore insufficient for authenticating legitimate manager requests.

¹⁶SNMP enables network and system administrators to remotely monitor and configure devices on the network (devices such as switches and routers).

Sensitive Information Was Not Always Encrypted

FDIC without a reliable trail to follow to hold the user accountable in the event of a security incident.

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of sensitive information. A basic element of cryptography is encryption.¹⁷ Encryption can be used to provide basic data confidentiality and integrity by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm.¹⁸ If encryption is not used, user ID and password combinations will be susceptible to electronic eavesdropping by devices on the network when they are transmitted. NSA and NIST recommend encrypting network services, and NIST guidance states that organizations should configure an information system to provide only the essential capabilities needed or restrict the use of protocols that can allow the unauthorized transfer of information.¹⁹ NIST guidance also states that the use of encryption by organizations can reduce the probability of unauthorized disclosure of information.

FDIC did not always ensure that sensitive information transmitted over its network was adequately encrypted. Specifically, FDIC did not disable an unencrypted protocol in use in the production and nonproduction logical partitions on the mainframe. In addition, FDIC did not restrict the use of unencrypted protocols on network servers. As a result, increased risk exists that an individual could capture information such as user IDs and passwords and use them to gain unauthorized access to data and system resources.

¹⁷Encryption is a subset of cryptography, which is used to secure transactions by providing ways to ensure data confidentiality (assurance that the information will be protected from unauthorized access), data integrity (assurance that data have not been accidentally or deliberately altered), authentication of the message's originator, electronic certification of data, and nonrepudiation (proof of the integrity and origin of data that can be verified by a third party).

¹⁸A cryptographic algorithm and key are used to apply cryptographic protection to data (e.g., encrypt the data or generate a digital signature) and to remove or check the protection (e.g., decrypt the encrypted data or verify the digital signature).

¹⁹A protocol is a set of rules or procedures for transmitting data between electronic devices, such as computers. In order for computers to exchange information, there must be a preexisting agreement as to how the information will be structured and how each side will send and receive it.

Audit and Monitoring of Security-Relevant Events Were Inadequate

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions have been taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail for determining the source of a transaction or attempted transaction and monitoring user activity. To be effective, organizations should (1) configure the software to collect and maintain a sufficient audit trail for security-relevant events; (2) generate reports that selectively identify unauthorized, unusual, and sensitive access activity; and (3) regularly monitor and take action on these reports. NIST guidance states that an organization should review and analyze information system audit records for indications of inappropriate or unusual activity, and should report the findings to designated organization officials. NIST guidance also states that organizations should track and monitor access by individuals who use elevated access privileges and that an organization should review and analyze information system audit records for indications of inappropriate or unusual activity, and should report the findings to designated organization officials.

FDIC did not always sufficiently review audit and monitoring of security-relevant events. For example,

- FDIC’s monitoring processes did not detect the existence of default installation user accounts on three UNIX servers.
- FDIC did not effectively monitor certain dataset access activity on the mainframe.
- FDIC mainframe logging controls were inappropriately configured, allowing the creation of large quantities of logged data for routine activities.

As a result of these deficiencies, increased risk exists that unauthorized activity or a policy violation would not be detected on FDIC systems and networks.

Weaknesses in Other Information System Controls Increased Risk

In addition to access controls, other important controls should be in place to ensure the confidentiality, integrity, and availability of an organization’s information. These controls include policies, procedures, and techniques for securely segregating incompatible duties, configuring information systems, and updating continuity documents. However, FDIC weaknesses

Incompatible Duties and Functions Were Not Adequately Segregated

in these areas have increased the risk of unauthorized use, disclosure, modification, or loss of information and information systems.

In addition to having access controls, an organization should have policies, procedures, and controls in place to appropriately segregate computer-related duties. Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby gain unauthorized access to assets or records. Often segregation of incompatible duties is achieved by dividing responsibilities among two or more organizational groups, which diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the other. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. FDIC policy on UNIX security states that development and production data shall be separated and access controlled such that application developers have access to only development areas (nonproduction) and application users have access to only production areas (nondevelopment).

FDIC did not always adequately segregate incompatible computer-related duties and functions. For example, FDIC developers are allowed access to both development and production UNIX servers. Allowing developers such access reduced FDIC's ability to achieve segregation of duties and increased the risk of unauthorized and unnecessary access to sensitive production data by individuals who do not require it to perform their job duties. As a result, increased risk exists that users could perform unauthorized system activities without detection.

Although Elements of Configuration Management Controls Existed, They Were Not Always Fully Implemented

Configuration management is another 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. An effective configuration management process includes procedures for identifying, documenting, and assigning unique identifiers (for example, serial number and name) to a system's hardware and software parts and subparts, generally referred to as configuration items, and evaluating and deciding whether to approve changes to a system's baseline configuration. In addition, vendor specification states that engineers will not develop, repair, maintain, or test the product software after a system reaches its end-of-life date. NIST guidance also states that

an organization should promptly install security-relevant software updates, such as patches.

FDIC has implemented some elements of a configuration management process. Specifically, it has documented policy and procedures for assigning unique identifiers and naming configuration items so that they can be distinguished from one another and for requesting changes to configuration items. FDIC has also developed a change request process and a baseline for its systems.

However, FDIC did not always implement key configuration management controls over its information system components. For example, FDIC had critical end-of-life systems that were not supported by their manufacturers, which indicates that patches or updates for emerging threats were no longer available. In addition, patch levels for third-party software running on two UNIX servers at FDIC were not current and an obsolete version of third-party software was running on a Windows server. As a result, increased risk exists that these FDIC systems will be exposed to unauthorized access or manipulation through the exploitation of known vulnerabilities that have not been patched or emergent vulnerabilities for which no known remedy exists.

Contingency Planning Documentation Was Incomplete or Had Incorrect Information

Contingency planning, which includes developing contingency, business continuity, and disaster recovery plans, should be performed to ensure that when unexpected events occur, essential operations can continue without interruption or can be promptly resumed, and that sensitive data are protected. NIST guidance states that organizations should develop and implement a contingency plan that describes activities associated with backing up and restoring the system after a disruption or failure. The plan should be updated and include information such as contact, resources, and description of files in order to restore the application in the event of a disaster. In addition, the plans should be tested to determine the plans' effectiveness and the organization's readiness to execute the plans. Officials should review the plan results and initiate corrective actions.

FDIC has developed contingency plans, business continuity plans, and disaster recovery plans and has also conducted testing on these plans. However, one contingency plan at the Virginia Square office contained incomplete information. Specifically, the contingency plan did not include information such as resources (servers, applications, network components, supplies, telecommunications, and databases) and technical information about databases, libraries, and guidance for restoring devices to operational order.

In addition, the business continuity plans at the Dallas office did not have correct information. Specifically, one of the plans was dated September 2005, and was created for a previous location. In addition, another plan had missing information. It listed a contact person for the headquarters security department who no longer worked there. Also, there was no contact information for the emergency management team.

At the time of our review, FDIC officials stated that they will update the contingency and continuity plans with the required information. Until FDIC maintains current contingency and continuity plans, increased risk exists that it will not be able to effectively recover and continue operations when an emergency occurs and its operations will be disrupted.

FDIC Had Not Fully Implemented Its Information Security Program

A key reason for the information security weaknesses is that although FDIC has made important progress in implementing its security program, it did not always fully complete key information security program activities. FDIC has provided employees with security awareness and security-specific training, and has implemented a system to track remedial action plans to ensure that deficiencies are mitigated in an effective and timely manner. However, FDIC did not always fully implement key information security program activities such as effectively developing and implementing security policies, and implementing an effective continuous monitoring program. Until all key elements of its information security program have been fully and consistently implemented, FDIC will not have sufficient assurance that its financial information and assets are adequately safeguarded from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

Security Policies and Procedures Were Not Always Developed, Documented, or Implemented

A key task in developing an effective information security program is to establish and implement risk-based policies, procedures, and technical standards that govern security over an agency's computing environment. If properly implemented, policies and procedures help reduce the risk that could come from unauthorized access or disruption of services. Because security policies and procedures are the primary mechanisms through which management communicates its views and requirements, it is important that these policies and procedures be established and documented. FISMA requires agencies to develop and implement policies and procedures to support an effective information security program. NIST has also issued security standards and related guidance to help entities implement security controls, including appropriate information security policies and procedures.

While FDIC has generated agencywide information security policy relating to access control and risk management, certain policies and procedures had not always been developed, documented, and implemented. For example,

- FDIC did not develop or document policies and procedures to prevent users from having inappropriate or incompatible access to multiple applications. For example, FDIC did not have policies and procedures to identify and govern the assignment of access privileges to combinations of systems that create logical access to data that is otherwise prevented by applications. As a result, a combination of access privileges assigned to individuals allowed for the circumvention of an accounting application's access controls. Additionally, FDIC did not develop or document technical controls in place to identify or prevent the assignment of such combinations of access privileges that expose the data associated with certain applications from access outside of the access controls implemented within the functions of those applications. As a result, individuals could inappropriately obtain access to data in certain applications.
- FDIC did not implement the policy requiring service and administrator user accounts on UNIX servers to change their passwords.
- FDIC did not implement the policy to have many of the mainframe IDs set with an "expire date."

Until these policies and procedures are fully developed, documented, and implemented, FDIC has reduced assurance that computing resources are consistently and effectively protected from inadvertent or deliberate misuse, including fraud or destruction.

Continuous Monitoring Efforts Were Not Always Sufficient

NIST states that a continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the state of the security of the information system. The implementation of a continuous monitoring program can result in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones, the three principal documents in the security authorization package. A rigorous and well-executed continuous monitoring program significantly reduces the level of

effort required for the reauthorization of the information system. FDIC policy states that in addition to performing system test and evaluation in support of ongoing certification and accreditation efforts, FDIC is to routinely test major applications and their components as part of the continuous monitoring program. The program is designed to identify the most commonly exploited application-level vulnerabilities that exist within the enterprise infrastructure.

FDIC's continuous monitoring efforts were not always sufficient. FDIC did not sufficiently (1) monitor users' inappropriate and excessive access privileges to a business application that supports resolution and receivership activities, (2) have the ability to reliably detect changes to powerful mainframe programs, and (3) test and verify that all system interfaces were properly configured for the new systems before putting them into production. FDIC has a continuous monitoring process; however, several of the vulnerabilities we identified with respect to FDIC's security over its information systems were not identified through FDIC's routine monitoring of access privileges, audit logs, and adherence to established policies and procedures. We identified numerous access control vulnerabilities that were not identified by the continuous monitoring program. These vulnerabilities resulted in significant reductions in FDIC's capability to maintain effective controls and to protect the confidentiality, integrity, and availability of its information systems and information. As a result, FDIC had limited assurance that computing resources were being consistently and effectively protected from inadvertent or deliberate misuse, including fraud or destruction.

FDIC Has Mitigated Previously Reported Weaknesses

Despite the newly identified weaknesses, FDIC has made progress in mitigating previously reported information security weaknesses. The corporation has mitigated all 10 of the information security weaknesses reported in our calendar year 2007 audit.²⁰ To its credit, the corporation has made improvements to the configuration management controls and aspects of its security management. For example, it maintained a full and complete requirements baseline for two systems and included key

²⁰GAO, *Information Security: FDIC Sustains Program but Needs to Improve Configuration Management of Key Financial Systems*, GAO-08-564 (Washington, D.C.: May 30, 2008).

information in a remedial action plan. In addition, FDIC has corrected the FDIC Inspector General findings from the 2009 report.²¹

Conclusions

FDIC had many new control weaknesses putting its systems at a higher level of vulnerability to internal threats. These weaknesses impair the corporation's ability to ensure the confidentiality, integrity, and availability of financial and sensitive information. The weaknesses also represent a significant deficiency in internal controls over the information systems and data used for financial reporting. Despite the newly identified weaknesses, FDIC has made progress in mitigating previously reported information security weaknesses.

Until FDIC (1) mitigates known information security weaknesses in access controls and other information system controls and (2) fully implements a comprehensive agencywide information security program that includes developing, documenting, and implementing security policies and implementing an effective continuous monitoring program, its financial and other sensitive information will remain at increased risk of unauthorized disclosure, modification, or destruction, and its management decisions may be based on unreliable or inaccurate information.

Recommendations for Executive Action

We recommend that the Chairman direct the Chief Information Officer to take the following two actions to enhance the corporation's information security program:

- develop and document policies and procedures for assigning access to systems and databases where application controls could be compromised, and
- complete the implementation of an effective continuous monitoring program to detect vulnerabilities.

We are also making 31 new recommendations to address 28 new findings in a separate report with limited distribution. These recommendations consist of actions to implement and correct specific information security

²¹FDIC Office of Inspector General, *Information Technology Controls in Support of the FDIC Fund's 2008 and 2007 Financial Statement Audit*, AUD-09-020 (Washington, D.C.: Aug. 17, 2009).

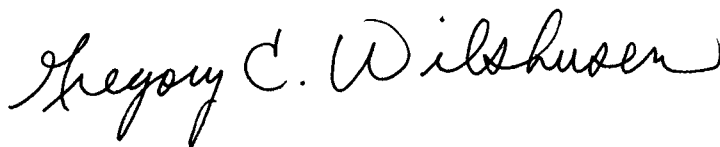
weaknesses related to access controls, segregation of duties, configuration management, and contingency planning identified during this audit.

Agency Comments

In providing written comments (reprinted in app. II) on a draft of this report, the Deputy to the Chairman and Chief Financial Officer of FDIC generally agreed with our recommendations. In addition, the Deputy discussed the actions that FDIC has taken or plans to take to implement the recommendations, such as restricting access to systems and databases and enhancing its continuous monitoring program as part of an ongoing multiyear effort.

We are sending copies of this report to the Chairman and Ranking Member of the Senate Committee on Banking, Housing, and Urban Affairs; Chairman and Ranking Member of the House Financial Services; members of the FDIC Audit Committee; the FDIC Inspector General; and other interested parties. In addition, this report will be available at no charge on the GAO Web site 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. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.



Gregory C. Wilshusen
Director, Information Security Issues



Dr. Nabajyoti Barkakati
Director, Chief Technologist

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to assess (1) the effectiveness of the Federal Deposit Insurance Corporation's (FDIC) controls in protecting the confidentiality, integrity, and availability of its financial systems and information, and (2) the progress FDIC has made in mitigating previously reported information security weaknesses. These objectives were integral to supporting our opinion on FDIC's internal controls provided in conjunction with our integrated audit of the financial statements of the two funds administered by FDIC, by assessing the controls over systems that support financial management and the generation of financial statements for two FDIC funds.

To determine whether controls over key financial systems were effective, we tested the effectiveness of information security and information technology-based internal controls. We concentrated our evaluation primarily on the controls for financial applications and enterprise database applications associated with a corporatwide system that functions as a unified set of financial and payroll systems that are managed together and operated in an integrated fashion; a system to calculate and collect FDIC deposit insurance premiums and Financing Corporation bond principal and interest amounts from insured financial institutions;¹ a Web-based application that provides full functionality to support franchise marketing, asset marketing, and asset management; a system to request access to and receive permission for the computer applications and resources available to its employees, contractors, and other authorized personnel; a primary receivership and subsidiary financial processing and reporting system; and the general support systems. Our selection of the systems was based on discussions with our stakeholders.

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

¹The 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 & 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.

Using National Institute of Standards and Technology (NIST) standards and guidance and FDIC's policies, procedures, practices, and standards, we evaluated controls by

- observing methods for providing secure data transmissions across the network to determine whether sensitive data were being encrypted;
- testing and observing physical access controls to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft;
- evaluating the control configurations of selected servers and database management systems;
- inspecting key servers and workstations to determine whether critical patches had been installed or were up-to-date; and
- examining access responsibilities to determine whether incompatible functions were segregated among different individuals.

Using the requirements of the Federal Information Security Management Act (FISMA), which establishes key elements for an effective agencywide information security program, we evaluated FDIC's implementation of its security program by

- reviewing FDIC's risk assessment process and risk assessments for key FDIC systems that support the preparation of financial statements to determine whether risks and threats were documented consistent with federal guidance;
- analyzing FDIC's policies, procedures, practices, and standards to determine their effectiveness in providing guidance to personnel responsible for securing information and information systems;
- analyzing security plans to determine if management, operational, and technical controls were in place or planned and that security plans were updated;
- examining training records for personnel with significant security responsibilities to determine if they had received training commensurate with those responsibilities;
- analyzing configuration management plans and procedures to determine if configurations were being managed appropriately;

- analyzing security testing and evaluation results for four key FDIC systems to determine whether management, operational, and technical controls were tested at least annually and based on risk;
- examining remedial action plans to determine whether they addressed vulnerabilities identified in FDIC's security testing and evaluations; and
- examining contingency plans for four key FDIC systems to determine whether those plans had been tested or updated.

We also discussed with key security representatives and management officials whether information security controls were in place, adequately designed, and operating effectively.

To determine the status of FDIC's actions to correct or mitigate previously reported information security weaknesses, we identified and reviewed its information security policies, procedures, and guidance. We reviewed prior GAO reports to identify previously reported weaknesses and examined FDIC's corrective action plans to determine which weaknesses FDIC had reported were corrected. For those instances where FDIC reported it had completed corrective actions, we assessed the effectiveness of those actions.

We conducted this performance audit from December 2009 to November 2010 in accordance with generally accepted government auditing standards. We performed our data collection, analysis, and assessment procedures in support of the financial audit during the December 2009 to June 2010 time frame. We performed supplemental audit procedures to prepare this report from June 2010 to November 2010. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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

November 19, 2010

Mr. Gregory C. Wilshusen
Director, Information Security Issues
Dr. Nabajyoti Barkakati
Director, Chief Technologist
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) draft audit report titled, Information Security: Federal Deposit Insurance Corporation Needs to Mitigate Control Weaknesses, GAO-11-29. We are pleased to accept GAO's acknowledgement of improvements FDIC has made in configuration management and aspects of security management as well as FDIC's correction of all information security weaknesses reported in prior years' financial statement audits.

The GAO's report contains two new recommendations to assist FDIC in further strengthening its information security controls. FDIC has reviewed these recommendations along with the accompanying statements of condition on which the recommendations are based. FDIC has taken action or will take action to restrict access to systems and databases and will continue to enhance its continuous monitoring program as part of an ongoing multi-year effort.

Specifically, GAO recommended that FDIC strengthen policies and procedures for assigning access to systems and databases where application controls could be compromised. FDIC agrees to implement the necessary improvements to ensure appropriate policies and procedures are documented and followed in assigning these types of access. FDIC will complete the necessary actions by March 31, 2011.

GAO further recommended that the FDIC strengthen its continuous monitoring program to detect vulnerabilities. FDIC recognizes that a continuous monitoring program, by its very nature, is an evolving program and will continue to build upon the processes now in place by targeting the highest risk areas. During 2010, the FDIC acquired additional automated monitoring tools which are currently being phased into our monitoring processes. In addition, by June 30, 2011, the FDIC will document our risk-based continuous monitoring program describing the current state and planned near-term improvements. Implementation will be performed in accordance with the plan and possible future guidance from the National Institute of Standards and Technology (NIST).

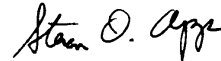
**Appendix II: Comments from the Federal
Deposit Insurance Corporation**

Mr. G. Wilshusen and Dr. N. Barkakati

November 19, 2010

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 2010 audit and beyond. If you have any questions relating to the FDIC management response, please contact James H. Angel, Jr., Director, Office of Enterprise Risk Management, at 703-562-6456.

Sincerely,



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

cc: Russell Pittman
Mitchell Glassman
Arleas Upton Kea
Bret Edwards
James H. Angel, Jr.
Audit Committee

- 2 -

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, David B. Hayes and Charles M. Vrabel (assistant directors), Nancy E. Glover, Mickie E. Gray, Rosanna Guerrero, Tammi N. Kalugdan, Duc M. Ngo, Zsaroq R. Powe, Eugene E. Stevens IV, and Henry I. Sutanto 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 Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to 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 Web site, <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.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@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, youngcl@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

