

August 2011

INFORMATION
SECURITY

Federal Deposit
Insurance Corporation
Has Made Progress,
but Further Actions
Are Needed to Protect
Financial Data

U.S. Government Accountability Office

GAO90

YEARS

1921-2011

ACCOUNTABILITY ★ INTEGRITY ★ RELIABILITY



Highlights of [GAO-11-708](#), a report to the Acting 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 FDIC's work, effective information security controls are essential to ensure that the corporation's systems and information are adequately protected from inadvertent misuse, fraudulent use, or improper disclosure.

As part of its audits of the 2010 financial statements of the Deposit Insurance Fund and the Federal Savings & 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 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 recommends that FDIC take two actions to enhance its comprehensive information security program. In commenting on a draft of this report, FDIC discussed actions that it has taken or plans to take to address these recommendations.

View [GAO-11-708](#) 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.

August 2011

INFORMATION SECURITY

Federal Deposit Insurance Corporation Has Made Progress, but Further Actions Are Needed to Protect Financial Data

What GAO Found

Although FDIC had implemented numerous controls in its systems, it had not always implemented access and other controls to protect the confidentiality, integrity, and availability of its financial systems and information. FDIC has implemented controls to detect and change default user accounts and passwords in vendor-supplied software, restricted access to network management servers, developed and tested contingency plans for major systems, and improved mainframe logging controls. However, the corporation had not always (1) required strong passwords on financial systems and databases; (2) reviewed user access to financial information in its document sharing system in accordance with policy; (3) encrypted financial information transmitted over and stored on its network; and (4) protected powerful database accounts and privileges from unauthorized use. In addition, other weaknesses existed in FDIC's controls that were intended to appropriately segregate incompatible duties, manage system configurations, and implement patches.

An underlying reason for the information security weaknesses is that FDIC had not always implemented key information security program activities. To its credit, FDIC had developed and documented a security program and had completed actions to correct or mitigate 26 of the 33 information security weaknesses that were previously identified by GAO. However, the corporation had not assessed risks, documented security controls, or performed periodic testing on the programs and data used to support the estimates of losses and costs associated with the servicing and disposal of the assets of failed institutions. Additionally, FDIC had not always implemented its policies for restricting user access or for monitoring the progress of security patch installation.

Because FDIC had made progress in correcting or mitigating previously reported weaknesses and had implemented compensating management and reconciliation controls during 2010, GAO concluded that FDIC had resolved the significant deficiency in internal control over financial reporting related to information security reported in GAO's 2009 audit, and that the remaining unresolved issues and the new issues identified did not individually or collectively constitute a material weakness or significant deficiency in 2010. However, if left unaddressed, these issues will continue to increase FDIC's risk that its sensitive and financial information will be subject to unauthorized disclosure, modification, or destruction.

Contents

Letter		1
	Background	3
	Opportunities Exist for FDIC to Improve Information Security Controls	7
	Conclusions	21
	Recommendations for Executive Action	21
	Agency Comments and Our Evaluation	22
Appendix I	Objective, Scope, and Methodology	24
Appendix II	Comments from the Federal Deposit Insurance Corporation	27
Appendix III	GAO Contacts and Staff Acknowledgments	29

Abbreviations

FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Management Act
ID	identification
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SAS	Statement on Auditing Standards
SSAE	Statement on Standards for Attestation Engagements
US-CERT	United States Computer Emergency Readiness Team
VPN	virtual private network

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

August 12, 2011

The Honorable Martin J. Gruenberg
Acting Chairman
Federal Deposit Insurance Corporation

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

As part of our audits of FDIC's calendar year 2010 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 FDIC had resolved the significant deficiency³ over information systems that we had reported 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' 2010 and 2009 Financial Statements*, [GAO-11-412](#) (Washington, D.C.: Mar. 18, 2011).

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 to detect and correct misstatements on a timely basis.

our 2009 audit, and that the unresolved prior year issues and new weaknesses we identified did not individually or collectively constitute a material weakness⁴ or a significant deficiency in internal controls over the information systems and data used for financial reporting for 2010 because the corporation had made improvements in its information security controls and had implemented compensating management and reconciliation controls to detect potential misstatements in the Deposit Insurance Fund. However, the weaknesses we identified, particularly those weaknesses associated with FDIC's process for deriving and reporting estimates of losses to the Deposit Insurance Fund from resolution transactions involving loss-sharing agreements, still present challenges for FDIC in ensuring that authorized users have only the access needed to perform their assigned duties and in adequately protecting corporate systems from unauthorized access.

In this report, we provide additional details on FDIC's information security controls over its computerized financial systems during calendar year 2010. Our objective was to determine the effectiveness of the corporation's controls protecting the confidentiality, integrity, and availability of its financial systems and information. This work was performed to support our opinion on FDIC's internal control over financial reporting as of December 31, 2010. We conducted this audit at FDIC facilities in Arlington, Virginia, and Washington, D.C., from November 2010 to August 2011, in accordance with generally accepted government auditing standards.⁵ Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe our audit provides a reasonable basis for our findings and conclusions. See appendix I for additional details on our objective, scope, and methodology.

⁴A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or will not be detected and corrected on a timely basis.

⁵We conducted data collection, analysis, and assessment procedures in support of the financial audit during the November 2010 to March 2011 time frame. We conducted supplemental audit procedures to prepare this report from March 2011 to August 2011.

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 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, their use also exposes FDIC's information to various internal and external threats.

Cyber-based threats to information systems and cyber-related critical infrastructure can come from sources internal and external to the organization. Internal threats include errors as well as fraudulent or malevolent acts by employees or contractors working within an organization. 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.

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 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 650 percent from fiscal year 2006 to fiscal year 2010. Specifically, the number of incidents reported by federal agencies to the United States Computer Emergency Readiness Team⁶ (US-CERT) has increased dramatically over the past 4 years: from 5,503 incidents reported in fiscal year 2006 to about 41,776 incidents in fiscal year 2010.

Compounding the growing number and kinds 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.

⁶The Department of Homeland Security's federal information security incident center is hosted by US-CERT. When incidents occur, agencies are to notify the center.

Accordingly, we have designated information security as a governmentwide high risk area since 1997, a designation that remains in force today.⁷ The Federal Information Security Management Act (FISMA)⁸ 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 1933⁹ in response to the thousands of bank failures that had occurred throughout the late 1920s and early 1930s.¹⁰ 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.¹¹ 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

⁷GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997) and *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

⁸FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

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

¹⁰FDIC is an independent agency of the federal government and receives no direct federal appropriations; it is funded by premiums that banks and thrift institutions pay for deposit insurance coverage and from earnings on investments in U.S. Treasury securities. Additionally, FDIC realizes some income from failed financial institutions for services it performs on their behalf.

¹¹Pub. L. No. 101-73, § 211, 103 Stat. 183, 218-22 (Aug. 9, 1989).

former Resolution Trust Corporation.¹² 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 2005.¹³

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 relies on many systems, including a corporatewide system that functions as a unified set of financial and payroll systems that are managed and operated in an integrated fashion, a system to calculate and collect FDIC deposit insurance premiums and Financing Corporation¹⁴ 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; 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.

¹²A 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.

¹³Pub. L. No. 109-171, Title II, Subtitle B, § 2102 (Feb. 8, 2006).

¹⁴The 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 noncallable bonds with a principal amount of approximately \$8.1 billion, mature in 2017 through 2019.

FDIC also relies on other computerized systems in deriving its estimates of losses from loss-sharing agreements.¹⁵ This complex estimation process was developed and implemented in order to manage the significant number of loss-sharing agreements that have been created as a result of the current financial crisis. The process uses databases containing information on loss-sharing agreements and asset valuations, software programs that use information from the databases and other sources to calculate the estimated losses, data and programs stored in FDIC's document sharing system, a Web service used to exchange valuation information with outside contractors, and several manual processing steps. In addition, in order to reduce the risk that a material misstatement will not be detected, FDIC relies heavily on supervisory review and oversight controls in the process. We have previously reported¹⁶ that this process is complex, is not fully documented, and involves multiple manual data entries. In a separate report,¹⁷ we have made an additional recommendation to FDIC to improve the documentation around this process.

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

¹⁵Under a loss-sharing agreement, FDIC sells a failed institution to an acquirer with an agreement that FDIC, through the Deposit Insurance Fund, will share in losses the acquirer experiences in servicing and disposing of assets purchased and covered under the loss-sharing agreement.

¹⁶[GAO-11-412](#).

¹⁷GAO, *Management Report: Opportunities for Improvements in FDIC's Internal Controls and Accounting Procedures*, GAO-11-687R (Washington, D.C.: Aug. 5, 2011).

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 the overall support of assessment and authorization activities;¹⁸ for the development, coordination, and implementation of FDIC's security policy; and for the coordination of information security and privacy efforts across the corporation.

Opportunities Exist for FDIC to Improve Information Security Controls

Although FDIC had implemented numerous controls over its systems, it had not always implemented access and other controls to protect the confidentiality, integrity, and availability of its financial systems and information. A key reason for these weaknesses is that the corporation did not always fully implement key information security program activities, such as effectively developing and implementing security policies. Although these weaknesses did not individually or collectively constitute a material weakness or significant deficiency in 2010, they still increase the risk that financial and other sensitive information could be disclosed or modified without authorization.

FDIC Had Not Always Restricted Access to Information Resources

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 system boundary protections, identification and authentication of users,

¹⁸The Office of Management and Budget (OMB) requires that a management official formally authorize an information system to process information and accept the risk associated with its operation based on a formal evaluation (or assessment) 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.

FDIC Had Not Always Protected System Boundaries

authorization restrictions, cryptography, protection of sensitive system resources, 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 for personal gain. In addition, authorized users could intentionally or unintentionally modify or delete data or execute changes that are outside of their authority.

Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from network-connected devices. Any connections to the Internet or to other external and internal networks or information systems should occur through controlled interfaces (for example, proxies, gateways, routers and switches, firewalls,¹⁹ and concentrators). Many networked systems allow remote access to the information systems from virtually any remote location; thus, it is imperative that remote access paths be appropriately controlled and protected using a method such as a virtual private network (VPN).²⁰ In addition, networks should also be appropriately configured to adequately protect access paths between systems; this can be accomplished through the use of access control lists and firewalls. National Institute of Standards and Technology (NIST) guidance states that agencies should establish trusted communication paths between users and the agency's information systems, that firewalls should be configured to provide adequate protection for the organization's networks, and that the information transmitted between interconnected systems should be controlled and regulated.

FDIC had not always controlled the logical and physical boundaries protecting its information and systems. Examples are as follows:

- Certain network devices, servers, and workstations on FDIC's internal network were not always configured to sufficiently restrict access or to fully secure connections.

¹⁹A firewall is a hardware or software component that protects computers or networks from attacks by blocking network traffic.

²⁰A VPN is a private network that is maintained across a shared or public network, such as the Internet, by means of specialized security procedures. VPNs are intended to provide secure connections between remote clients, such as branch offices or traveling personnel and a central office.

-
- Firewalls controlling traffic between segments of FDIC’s internal network did not sufficiently control certain types of network traffic.
 - Boundary protection controls were configured in a manner that limited the effectiveness of monitoring controls.

As a result of these deficiencies, FDIC faces an increased risk that individuals could gain unauthorized access to its financial systems and information.

Controls for Identifying and Authenticating Users 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 the system from inadvertent or malicious access. When an organization assigns a unique user account to a specific user, the system is able to distinguish that user from others—a process called identification. The system must also establish the validity of the user’s claimed identity by requesting some kind of information, such as a password, which is known only by the user—a process called authentication. 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. Also, FDIC policy states that passwords should be changed periodically.

FDIC had effectively implemented controls for identifying and authenticating users on certain systems. For example, it had implemented controls to effectively detect and change default vendor-supplied user accounts and passwords in installed software and had ensured that passwords for privileged accounts on certain servers were changed in accordance with its policy.

However, FDIC had not consistently enforced other identification and authentication user controls. Examples are as follows:

- Passwords for certain privileged accounts on a system supporting financial processing were not configured in accordance with FDIC policy. Additionally, two of the accounts were using the same password.
- Password settings for certain accounts on a system supporting the loss-share loss estimation process were not configured in accordance with FDIC policy.

-
- Systems supporting financial processing were not always configured with sufficiently strong identification and authentication controls.

As a result of these deficiencies, FDIC is at an increased risk that an individual with malicious intentions could gain inappropriate access to its financial systems and information.

FDIC Had Implemented Restrictions on User Access, but Weaknesses Still Exist

Authorization is the process of granting or denying access rights and privileges to a protected resource, such as a network, system, application, function, or file. A key component of granting or denying access rights is the concept of “least privilege,” which refers to granting a user only the access rights and permissions needed to perform official duties. To restrict a legitimate user’s access to only those programs and files needed, organizations establish user access rights: allowable actions that can be assigned to a user or to groups of users. File and directory permissions are rules that are associated with a particular file or directory, regulating which users can access it—and the extent of their access rights. To avoid unintentionally giving a user unnecessary access to sensitive files and directories, an organization should give careful consideration to its assignment of rights and permissions. NIST guidance states that access to information systems should be allowed only for authorized users and only for the tasks necessary to accomplish the work, in accordance with the organization’s missions and business functions. In addition, NIST guidance states that agency information systems should separate user functionality from functions necessary to administer databases, network components, workstations, or servers. FDIC policy requires that the access to information technology (IT) resources be periodically reviewed to ensure that access controls remain consistent with existing authorizations and current business needs. Also, the Division of Resolutions and Receiverships requires user access to the document sharing system supporting the loss-share estimation process to be reviewed every 3 months.

FDIC had implemented controls to restrict user access to certain resources. For example, it had configured access control lists on servers dedicated to network management to restrict access to only those users who required it, controlled access to sensitive files of critical network devices, and limited user access rights to a business application supporting resolution and receivership activities to only those roles necessary for personnel to perform their duties.

However, other deficiencies in authorization controls placed FDIC’s financial information and systems at risk. Examples are as follows:

-
- The Division of Resolutions and Receiverships had not documented a procedure describing how access to the Web service used in the loss-share loss estimation process was to be reviewed, including requirements for conducting reviews at regular intervals or retaining documentation of reviews.
 - The Division of Resolutions and Receiverships had not reviewed access to the document sharing system every 3 months in accordance with its policy; instead, it had conducted a review only once during 2010.
 - FDIC had given users access to sensitive resources on certain systems supporting financial processing that they did not need to accomplish their work.

As a result, FDIC faces an increased risk 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.

Sensitive Information Was Not Always Encrypted

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of sensitive information. A basic element of cryptography is encryption.²¹ 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.²² If encryption is not used, user identification (ID) and password combinations will be susceptible to electronic eavesdropping by devices on the network when they are transmitted. The National Security Agency and NIST recommend encrypting network services, and NIST guidance states that passwords should be encrypted while being stored and transmitted. NIST guidance also states that the use of encryption by organizations can reduce the probability of unauthorized disclosure of

²¹Encryption 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).

²²A 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).

information and that government systems should use sufficiently strong encryption in order to establish and maintain secure communication links between information systems and applications.

FDIC had implemented controls to encrypt certain sensitive information on its systems. For example, it had restricted the use of unencrypted protocols on the mainframe and had required that sensitive information stored on user workstations or mobile devices be encrypted.

However, FDIC had not always ensured that sensitive financial information transmitted over and stored on its network was adequately encrypted. Specifically, FDIC had not always used sufficiently strong encryption on two systems supporting the loss-share loss estimation process and had not always strongly encrypted stored passwords on certain financial systems. As a result of these deficiencies, FDIC is at an increased risk that an individual could capture information such as user IDs and passwords and use them to gain unauthorized access to data and system resources.

Audit and Monitoring of Security-Relevant Events Was Not Always Adequate

To establish individual accountability, monitor compliance with security policies, and investigate security violations, the capability to determine what, when, and by whom specific actions have been taken on a system is needed. 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 by 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 organizations should track and monitor access by individuals who use elevated access privileges, review and analyze information system audit records for indications of inappropriate or unusual activity, and report the findings to designated organization officials.

FDIC had ensured that default installation user accounts were no longer used on certain servers and had configured its mainframe logging controls efficiently. However, FDIC's audit and monitoring of security-relevant events on key financial systems was not always sufficient. For example, FDIC had not always sufficiently configured logging controls on a system that supported the loss-share loss estimation process or on several network devices. As a result of these deficiencies, FDIC faces an

increased risk that unauthorized activity or a policy violation on its systems and networks would not be detected.

Other Information System Controls Can Be Improved

In addition to access controls, organizations should use policies, procedures, and techniques for securely segregating incompatible duties, configuring information systems, and ensuring continuity of computer processing operations in the event of a disaster or unexpected interruption to ensure the confidentiality, integrity, and availability of its information. However, FDIC's systems were not always in full compliance with these policies, procedures, and techniques, leaving them vulnerable to intrusions.

Incompatible Duties and Functions Were Not Adequately Segregated

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. According to NIST, in order to maintain separation of duties, personnel who administer access control functions should not also be responsible for administering audit functions.

FDIC's Division of Resolutions and Receiverships had not always separated audit responsibilities from administration of access to loss-share and asset valuation data and programs. Specifically, the FDIC access administrators for both the external Web service and the document sharing system used in the loss-share loss estimation process were also responsible for approving and reviewing user access to the systems. As a result, the access administrators had the ability to grant inappropriate levels of access to loss-share and asset valuation data and programs without being detected, placing the data and programs at risk of unauthorized access, misuse, modification, or destruction.

Elements of Configuration Management Controls Existed but Were Not 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 (1) 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; (2) evaluating and deciding whether to approve changes to a system's baseline configuration; (3) documenting and reporting on the status of configuration items as a system evolves; (4) determining alignment between the actual system and the documentation describing it; and (5) developing and implementing a configuration management plan for each system. In addition, establishing controls over the modification of information system components and related documentation helps to prevent unauthorized changes and ensure that only authorized systems and related program modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all hardware, software, and firmware programs and program modifications are properly authorized, tested, and approved.

According to NIST, organizations should document approved configuration-controlled changes to information systems, retain and review records of the changes, audit activities associated with the changes, and coordinate and provide oversight for configuration change control activities through a mechanism such as a change control board. NIST also recommends that agencies configure their systems to reflect the most restrictive mode possible consistent with operational requirements and employ malicious code protection mechanisms to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, or other common means.

FDIC had not applied appropriate configuration management controls to many of the special purpose programs and data in the loss-share estimating process. Although FDIC had documented activities for development, testing, and production for three of the programs used to calculate the estimates of losses due to loss-sharing agreements and had assigned responsibility for the different activities, it had neither documented approved changes to the programs prior to implementation nor retained records of the changes made. While the corporation had documented plans for tracking changes to these three programs, the plans had not been implemented. Additionally, the corporation had not documented plans for controlling changes to a program that generated a key dataset or to two other programs used to validate the data contained in a key database used in the loss-share loss estimation process. Furthermore, FDIC had not applied version control or change control to the database for the loss-share cost estimates. Moreover, a workstation

Critical Systems Were Not Always Fully Patched

used to execute one of the key calculation programs had configuration weaknesses that could allow it to be compromised. Until FDIC fully implements configuration management and configuration change controls to these data and programs, increased risk exists that changes to the programs could be unnecessary, may not work as intended, or may result in the unintentional loss of data or program integrity, or that individuals, both internal and external to the corporation, could exploit configuration weaknesses and gain unauthorized access to financial or other sensitive data and systems.

Patch management is a critical process that can help alleviate many of the challenges in securing computing systems.²³ Malicious acts can range from defacing a Web site to taking control of an entire system, thereby being able to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other organizations' systems. After a vulnerability has been validated, the software vendor may develop and test a patch or workaround to mitigate the vulnerability. Incident response groups and software vendors issue regular information updates on the vulnerability and the availability of patches. NIST guidance states that a comprehensive patch management process should include prioritization of the order in which vulnerabilities are addressed, with a focus on high-priority systems such as those essential for mission-critical operations.

FDIC had patched many of its systems and had ensured that much of its software was up-to-date. For example, it had retired critical network devices that were not supported by their manufacturers, updated patch levels for third-party software running on two UNIX servers, and removed an obsolete version of third-party software running on a Windows server.

However, FDIC had not consistently updated its financial systems and servers with critical patches or kept its software up-to-date, including systems supporting the loss-share loss estimation process. For example, certain servers supporting financial processing were running a version of software that was unsupported for patch updates, and several workstations used in the loss-share loss estimation process were missing patches and were running software that was no longer supported by the manufacturer. Additionally, certain workstations were missing operating

²³For example, see GAO, *Information Security: Continued Action Needed to Improve Software Patch Management*, [GAO-04-706](#) (Washington, D.C.: June 2, 2004).

Contingency Plans Were Not Documented for Systems and Processes Supporting Loss-Share Loss Estimation

system patches. As a result of these deficiencies, FDIC is at an increased risk that unpatched vulnerabilities could allow its information and information systems to be compromised.

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 contingency plans that describe activities associated with backing up and restoring the system after a disruption or failure. The plans 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 their effectiveness and the organization's readiness to execute the plans. Officials should review the test results and initiate corrective actions. FDIC's *Information Technology Security Risk Management Program* requires contingency plans and disaster recovery plans to be developed and tested for all sensitive applications (both major and nonmajor) and general support systems; the plans should address measures to be taken in response to a disruption in availability due to an unplanned outage.

Although FDIC had developed contingency plans for its major systems and had also conducted testing on these plans, it had not documented plans for recovering the automated and semiautomated processes supporting the loss-share loss estimation process. Although the security plan for one of FDIC's general support systems included the document sharing system and one of the key databases supporting the process, the corporation had not documented or tested contingency plans that addressed restoring the computer programs, workstations, and datasets supporting the preparations of the estimates of losses and costs due to loss-sharing agreements or of the workspaces within the document sharing system where loss-share and asset valuation information and programs are stored. As a result, FDIC may not be able to effectively recover the data and programs in the loss-share loss estimation process and resume normal operations after a disruption.

FDIC Had Not Always Implemented Key Activities of its Information Security Program

An underlying reason for the information security weaknesses noted in the previous section is that, while FDIC has developed and documented a comprehensive corporate information security program, including documenting an information security risk management policy, developing security policies and procedures, documenting system security plans, and periodically testing information security controls, the corporation had not fully implemented its information security program. Specifically, it had not fully implemented its security policies and had not completed actions to remediate certain control weaknesses. In addition, FDIC had not applied security management controls to the programs and data in the loss-share loss estimation process.

Security Program Elements Had Been Developed and Documented, but Not All Elements Had Been Fully Implemented

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

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;
- 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;
- plans for providing adequate information security for networks, facilities, and systems;
- 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; and

-
- a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in its information security policies, procedures, or practices.

FDIC had developed and documented a comprehensive corporate information security program that was consistent with FISMA requirements and had implemented some elements of its program, but had not fully implemented other elements. Specifically:

- FDIC had developed and documented an IT security risk management policy that required all sensitive applications to periodically be assessed for the risk and magnitude of harm that could result from vulnerabilities and potential threats.
- FDIC had not fully implemented its policies requiring that users be provided with only the minimum level of access required to allow them to perform their duties and that its computer security information response team monitor the progress of security patching activities by reviewing reports on the status of implementation. In addition, it had not fully implemented its policies for frequency of password changes and for storage of passwords.
- FDIC had developed and documented security plans for all of the major systems we reviewed that addressed policies and procedures for providing management, operational, and technical controls, and had documented requirements for physically securing FDIC facilities.
- FDIC had conducted annual periodic testing and evaluation of the effectiveness of the management, operational, and technical controls for the major systems we reviewed.
- Although FDIC had established a process for planning, implementing, evaluating, and documenting remedial actions to address information security weaknesses, and had completed actions to remediate 26 of the 33 control weaknesses we identified in our calendar year 2009 audit, the corporation had not yet completed actions to correct or mitigate 7 of the previously reported weaknesses. For example, FDIC had not separated or partitioned the data network from the voice network, developed and documented policies and procedures for assigning access to systems and databases where application controls could be compromised, or fully implemented its monitoring program.

In addition, FDIC had not received an independent audit report from the provider of its Web service in a timely manner. FISMA information security requirements apply not only to an agency's own systems but also to information systems used or operated on its behalf by a contractor or other agency, such as an external service provider. According to OMB,²⁴ service providers are required to provide client organizations with an audit report that describes whether internal controls were designed to achieve specified objectives, have been placed into operation, and are operating effectively. Previously known as Statement on Auditing Standards (SAS) 70 reports, since June 15, 2011, they have been known as Statement on Standards for Attestation Engagements (SSAE) 16 reports.²⁵ OMB also states that such reports should be provided within a reasonable time frame so that auditors of client organizations may use them during their financial statement audits. However, the provider of the Web service used to exchange information with valuation contractors did not provide FDIC with a SAS 70 report until March 2011, more than 8 weeks after the end of the financial reporting period and more than 5 months after the end of the period that the SAS 70 audit covered.

Until all key elements of its information security program are fully implemented, FDIC may not have assurance that controls over its financial systems and information are appropriately designed and operating effectively.

FDIC Had Not Applied Security Program Controls to the Loss-Share Loss Estimation Process

FDIC had not applied key controls in its information security program to the loss-share loss estimation process. OMB Circular A-130, Appendix III,²⁶ requires federal agencies to implement and maintain an automated information security program, including planning for adequate security of each system, assessing risks, and reviewing security controls. OMB

²⁴OMB, *Audit Requirements for Federal Financial Statements*, OMB-07-04 (Washington, D.C.: amended Sept. 23, 2009).

²⁵SSAE 16 reports refer to reports typically prepared by an independent auditor based on a review of the controls relevant to user entities' internal control over financial reporting as discussed in the American Institute of Certified Public Accountants' Statement on Standards for Attestation Engagements (SSAE) No. 16, *Reporting on Controls at a Service Organization*. A service organization provides services to the entity whose financial statements are being audited.

²⁶OMB, Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources* (Washington, D.C.: Nov. 28, 2000).

Circular A-127²⁷ requires that federal financial management systems, which include core financial systems as well as any automated and manual processes, procedures, data, hardware, and software that support financial management, be subject to the requirements of Circular A-130. However, FDIC had not applied key controls in its information security program to the automated and semiautomated processes used to support the preparation of the estimates of losses and costs due to loss-sharing agreements. Specifically, FDIC had not

- assessed the risks associated with the information and programs involved to identify potential threats and vulnerabilities as well as possible countermeasures and mitigating controls, and had not included the programs in the risk assessment of any of its general support systems;
- documented the management, technical, or operational security controls intended to protect the programs in system security plans, and had not included the programs in the system security plans of any general support system; or
- tested any security controls for the programs, and had not included the programs when testing the security controls of other general support systems.

FDIC had not applied these controls because the Division of Resolutions and Receiverships developed the process independently, in order to be able to manage the large increase in bank failures and the extensive use of loss-sharing agreements resulting from the current financial crisis. In doing so, the Division of Resolutions and Receiverships had not used FDIC's existing IT management framework—which requires these controls to be put into place—to develop and manage the process.

During 2010, FDIC had mitigated the effect of these weaknesses on financial reporting by implementing compensating management and reconciliation controls in this process. However, because of ongoing financial institution failures and the lack of information security management controls around the process, the financial information processed by the programs involved—representing a nearly \$39 billion

²⁷OMB, Circular No. A-127, *Financial Management Systems* (Washington, D.C.: Jan. 9, 2009).

impact on the corporation's financial statements—continues to be at risk of unauthorized disclosure, modification, or destruction.

Conclusions

FDIC has made significant progress in correcting or mitigating previously reported information security weaknesses, but other control weaknesses continue to unnecessarily put FDIC's systems at an increased risk from internal and external threats. A key reason for these weaknesses is that the corporation had not fully implemented key elements of its information security program, such as effectively implementing security policies, conducting risk assessments, documenting security management plans, documenting contingency plans, testing security controls, or implementing an effective continuous monitoring program. FDIC had made improvements in its information security controls and had mitigated the potential effect of its remaining weaknesses on financial reporting by implementing compensating management and reconciliation controls during 2010, enabling us to conclude that FDIC had resolved the significant deficiency over information systems that we had reported in our 2009 audit. However, the weaknesses—both old and new—continue to challenge the corporation in its efforts to ensure the confidentiality, integrity, and availability of financial and sensitive information.

Until FDIC further mitigates known information security weaknesses in access controls and other information system controls and fully implements its information security program, the corporation will continue to face an increased risk that sensitive financial information and resources will not be sufficiently protected from inadvertent or deliberate misuse, improper disclosure, or destruction.

Recommendations for Executive Action

We recommend that the Acting Chairman take the following two actions to enhance FDIC's information security program:

- Direct the Director of the Division of Resolutions and Receiverships and the Chief Information Officer to develop, document, and implement appropriate information security activities in the loss-share loss estimation process, such as assessing and mitigating risks, managing and controlling the configurations of programs and databases, evaluating the effectiveness of security controls, and ensuring that data and programs can be recovered after a disruption.
- Direct the Chief Information Officer to work with the external Web service provider to obtain a more timely delivery of the provider's

SSAE 16 report (previously known as a SAS 70 report), or to obtain other means of assurance of internal controls.

We are also making 38 new recommendations to address 37 new findings in a separate report with limited distribution. These recommendations consist of actions to implement and correct specific information security weaknesses related to access controls, segregation of duties, configuration management, and contingency planning identified during this audit.

Agency Comments and Our Evaluation

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 stated that FDIC was pleased to accept our acknowledgment of the significant progress made toward correcting and mitigating our previously reported weaknesses. In addition, he indicated that the corporation plans to implement improvements to address our recommendations, and discussed the actions that FDIC has taken or plans to take to review and improve controls over the loss-share loss estimation process, to obtain timely delivery of appropriate audit reports from current and future service providers, and to conduct additional due diligence activities to obtain assurance of the service provider's internal controls.

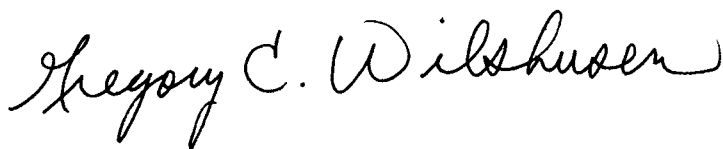
In responding to our draft recommendation that FDIC develop, document, and implement appropriate information security controls over the automated and semiautomated processes within the loss-share loss estimation process, the Deputy to the Chairman stated that although FDIC agrees that the loss-share business processes and the data associated with these processes deserve proper controls assessment and protection, the corporation will not necessarily treat the processes and data as a separate FDIC system. The Deputy to the Chairman further stated that FDIC is currently taking steps to improve the information security controls around the process.

The intent of our draft recommendation was not to suggest that FDIC treat the data and programs supporting the loss-share loss estimation process as a separate information system. We agree that it may not be appropriate for FDIC to treat these data and programs as a separate information system, as they are stored, processed, and executed across multiple systems. Rather, our intent was to recommend that appropriate information security control activities be incorporated into the process. Accordingly, we have clarified our recommendation to state that the Acting Chairman direct the Director of the Division of Resolutions and

Receiverships and the Chief Information Officer to develop, document, and implement appropriate information security activities in the loss-share loss estimation process, such as assessing and mitigating risks, managing and controlling the configurations of programs and databases, evaluating the effectiveness of security controls, and ensuring that data and programs can be recovered after a disruption.

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 Committee; 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. Key contributors to this report are listed in appendix III.



Gregory C. Wilshusen
Director, Information Security Issues



Dr. Nabajyoti Barkakati
Director, Center for Technology and Engineering

Appendix I: Objective, Scope, and Methodology

The objective of our audit was to determine the effectiveness of the Federal Deposit Insurance Corporation's (FDIC) controls 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 key financial applications; and interviewed key 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 the preparation of the calendar year 2010 and 2009 financial statements of two funds administered by FDIC.

To determine whether controls over key financial systems were effective, we considered the results of our evaluation of FDIC's actions to mitigate previously reported weaknesses and performed new audit work at FDIC facilities in Arlington, Virginia, and Washington, D.C. We concentrated our evaluation primarily on the controls for financial applications and enterprise database applications associated with the New Financial Environment; the Assessment Information Management System; the Communication, Capability, Challenge, and Control System (4C) application; the programs, data, and systems supporting the preparation of the estimates of losses and costs due to loss-sharing agreements, and the general support systems. Our selection of the systems to evaluate was based on consideration of systems that directly or indirectly support the processing of material transactions that are reflected in the funds' financial statements.

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

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

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 reported as being corrected. For those instances where FDIC reported it had completed corrective actions, we assessed the effectiveness of those actions.

We conducted this audit from November 2010 to August 2011, in accordance with generally accepted government auditing standards. We conducted our data collection, analysis, and assessment procedures in support of the financial audit between November 2010 and March 2011. We conducted supplemental audit procedures to prepare this report from March 2011 to August 2011. The generally accepted government auditing standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

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

July 21, 2011

Mr. Gregory C. Wilshusen
Director, Information Security Issues
Dr. Nabajyoti Barkakati
Director, Center for Technology and Engineering
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 Has Made Progress, but Further Actions Are Needed to Protect Financial Data, GAO-11-708. We are pleased to accept GAO's acknowledgement of significant progress FDIC has made correcting and mitigating previously reported information security weaknesses.

The GAO's report contains two new recommendations to assist FDIC in further strengthening its information security controls. FDIC will implement improvements to address these recommendations.

Specifically, GAO recommended that FDIC develop, document, and implement appropriate information security controls, such as configuration management and configuration change controls, contingency plans, risk assessments, security plans, and testing and evaluation plans, in the automated and semi-automated processes within the loss share loss estimation process. The FDIC takes seriously the GAO's concerns regarding loss share related controls as evidenced by improvements in those controls during 2010. The FDIC agrees that the loss share business processes and the data associated with these processes deserve proper control assessment and protection. Nevertheless, FDIC will not necessarily treat these processes and associated data as a separate FDIC system. Consistent with the progress of our review of the appropriate controls over these automated and semi-automated processes, FDIC is currently taking steps to improve role-based access control, data integrity, and configuration management (i.e. version control) on data repositories and shared network resources that contain end-user commodity tools used to augment the loss share estimation processes. The process to review and improve controls began while the GAO audit team was on site and will continue through December 2011.

Further, GAO recommended that FDIC work with the external Web service provider to obtain a more timely delivery of the provider's SSAE 16 report (previously known as a SAS 70 report), or to obtain other means of assurance of internal controls. FDIC will work with current and future outsourced information service providers to obtain timely delivery of the appropriate Service Organization Control (SOC) reports for annual review. FDIC will also continue to

Appendix II: Comments from the Federal
Deposit Insurance Corporation

Mr. G. Wilshusen and Dr. N. Barkakati

July 21, 2011

conduct additional due diligence activities to obtain assurance of the service provider's internal controls. These activities may include obtaining an assertion letter from the service provider's management regarding whether or not controls have changed since the last review. They may also include obtaining supplemental information regarding any changes in the design and operation of the service provider's internal controls and supporting processes.

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 2011 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: James H. Angel, Jr.
Bret Edwards
Craig Jarvill
Russell Pittman
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, Lon Chin, David Hayes, Charles Vrabel, and Christopher Warweg, Assistant Directors; Gary Austin; Angela Bell; William Cook; Saar Dagani; Nancy Glover; Rosanna Guerrero; Jason Porter; Michael Stevens; and Shaunyce Wallace 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, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

