

GAO

Report to the Chief Financial Officer
and Chief Operating Officer, Federal
Deposit Insurance Corporation

May 2008

INFORMATION SECURITY

FDIC Sustains Progress but Needs to Improve Configuration Management of Key Financial Systems





Highlights of [GAO-08-564](#), a report to the Chief Financial Officer and Chief Operating Officer, 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. Effective information security controls are essential to ensure that FDIC systems and information are adequately protected from inadvertent misuse, fraudulent, or improper disclosure.

As part of its audit of FDIC's 2007 financial statements, GAO assessed (1) the progress FDIC has made in mitigating previously reported information security weaknesses and (2) the effectiveness of FDIC's controls in protecting the confidentiality, integrity, and availability of its financial systems and information. To do this, GAO examined security policies, procedures, reports, and other documents; observed controls over key financial applications; and interviewed key FDIC personnel.

What GAO Recommends

GAO recommends that FDIC take actions to improve access and configuration management controls and to perform key information security program activities for two financial systems. FDIC concurred with one and partially concurred with nine of GAO's recommendations and has developed or implemented plans to address these recommendations. In some instances, FDIC chose to pursue alternative corrective actions. If the corporation effectively implements these alternative actions to reduce risk, it will satisfy the intent of our recommendations.

To view the full product, including the scope and methodology, click on [GAO-08-564](#). 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.

INFORMATION SECURITY

FDIC Sustains Progress but Needs to Improve Configuration Management of Key Financial Systems

What GAO Found

FDIC has made significant progress in mitigating previously reported information security weaknesses. Specifically, it has corrected or mitigated 16 of the 21 weaknesses that GAO had previously reported as unresolved at the completion of the 2006 audit. For example, FDIC has improved physical security controls over access to its Virginia Square computer processing facility, instructed personnel to use more secure e-mail methods to protect the integrity of certain accounting data transferred over an internal communication network, and updated the security plan and contingency plan of a key financial system. In addition, FDIC stated it has initiated and completed some actions to mitigate the remaining five prior weaknesses. However, we have not verified that these actions have been completed.

Although FDIC has made significant progress improving its information system controls, old and new weaknesses could limit the corporation's ability to effectively protect the confidentiality, integrity, and availability of its financial systems and information. In addition to the five previously reported weaknesses that remain unresolved, newly identified weaknesses in access controls and configuration management controls introduce risk to two key financial systems. For example, FDIC did not always implement adequate access controls. Specifically, multiple FDIC users shared the same login ID and password, had unrestricted access to application source code, and used passwords that were not adequately encrypted. In addition, FDIC did not adequately (1) maintain a full and complete baseline for system requirements; (2) assign unique identifiers to configuration items; (3) authorize, document, and report all configuration changes; and (4) perform configuration audits. Although these weaknesses do not pose significant risk of misstatement of the corporation's financial statements, they do increase preventable risk to the corporation's financial systems and information. A key reason for these weaknesses is that FDIC did not always fully implement key information security program activities. For example, it did not adequately conduct configuration control testing or complete the remedial action plan in a timely manner and did not include necessary and key information. Until FDIC fully performs key information security program activities, its ability to maintain adequate control over its financial systems and information will be limited.

Contents

Letter		1
	Results in Brief	2
	Background	4
	FDIC Has Made Significant Progress Mitigating Previously Reported Weaknesses	8
	Weaknesses Continue to Reduce the Security of Financial Information	9
	Conclusions	21
	Recommendations for Executive Action	21
	Agency Comments and Our Evaluation	22
Appendix I	Objectives, Scope, and Methodology	24
Appendix II	Status of Previously Reported Weaknesses	27
Appendix III	Comments from the Federal Deposit Insurance Corporation	29
Appendix IV	GAO Contacts and Staff Acknowledgments	31
Tables		
	Table 1: NFE Does Not Have Unique Identifiers for the Same Requirement	14
	Table 2: AIMS II Does Not Have Unique Identifiers for the Same Requirement	15
	Table 3: AIMS II RequisitePro Requirements on the Traceability Matrix Do Not Match the Software Requirements Specification	16

Abbreviations

AIMS II	Assessment Information Management System II
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CMMI	Capability Maturity Model® Integration
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
NFE	New Financial Environment
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SRS	Software Requirement Specification
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.



United States Government Accountability Office
Washington, DC 20548

May 30, 2008

The Honorable Steven O. App
Deputy to the FDIC Chairman and Chief Financial Officer
Federal Deposit Insurance Corporation

The Honorable John F. Bovenzi
Deputy to the FDIC Chairman and Chief Operating Officer
Federal Deposit Insurance Corporation

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 sensitive information maintained on its systems—such as personnel and regulatory information—are of paramount concern. In particular, effective information security controls¹ are essential to ensure that FDIC systems and information are adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

As part of our audit of the calendar year 2007 financial statements of the Deposit Insurance Fund² and the Federal Savings & Loan Insurance Corporation Resolution Fund,³ we assessed (1) the progress FDIC has

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.

²The Bank Insurance Fund and the Savings Association Insurance Fund merged to become the Deposit Insurance Fund.

³GAO, *Financial Audit: Federal Deposit Insurance Corporation Funds' 2007 and 2006 Financial Statements*, GAO-08-416 (Washington, D.C.: Feb. 11, 2008).

made in mitigating previously reported information security weaknesses⁴ and (2) the effectiveness of FDIC's controls in protecting the confidentiality, integrity, and availability of its financial systems and information.

In our audit report⁵ of the calendar year 2007 financial statements for FDIC's funds, we concluded that issues related to information security controls did not constitute a significant deficiency in internal controls with respect to financial reporting and compliance with laws and regulations.⁶ We also stated in the report that continued management commitment to an effective information security program will be essential to ensuring that the corporation's financial systems and information will be adequately protected.

We performed our audit work from October 2007 to May 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. See appendix I for additional details on our objectives, scope, and methodology.

Results in Brief

FDIC has made significant progress in mitigating previously reported information security weaknesses. Specifically, it has corrected or mitigated 16 of the 21 weaknesses that we had previously reported as unresolved at the completion of the 2006 audit. For example, FDIC has improved physical security controls over access to the Virginia Square computer processing facility, instructed personnel to use more secure e-mail methods to protect the integrity of certain accounting data

⁴GAO, *Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress Improving Its Program*, [GAO-07-351](#) (Washington, D.C.: May 18, 2007).

⁵[GAO-08-416](#).

⁶A significant deficiency is a control deficiency, or combination of deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected.

transferred over an internal communication network, updated the security plan of a key financial system called the New Financial Environment (NFE) to clearly identify all common security controls, developed procedures to report computer security incidents, and updated the NFE contingency plan. However, FDIC has not yet completed actions to

- effectively generate NFE audit reports;
- maintain a complete listing of all NFE configuration items, including application software, data files, software development tools, hardware, and documentation;
- properly segregate incompatible system-related functions, duties, and capacities for an individual associated with the NFE;
- effectively implement or accurately report the status of its remedial actions; and
- properly update the NFE risk assessment.

FDIC stated it has initiated and completed some actions to mitigate the remaining five prior year weaknesses. However, we have not verified that these actions have been completed. Although FDIC has made significant progress improving its information system controls, old and new weaknesses could limit the corporation's ability to effectively protect the confidentiality, integrity, and availability of its financial systems and information. In addition to the five previously reported weaknesses that remain unresolved, newly identified weaknesses in access controls and configuration management controls introduce risk to two key financial systems. For example, FDIC did not always implement adequate access controls. Specifically, multiple FDIC users shared the same login ID and password, had unrestricted access to application source code, and used a password that was not adequately encrypted. In addition, FDIC did not adequately (1) maintain a full and complete baseline for system requirements; (2) assign unique identifiers to configuration items; (3) authorize, document, and report all configuration changes; and (4) perform configuration audits. Although these weaknesses do not pose a significant risk of material misstatement of the corporation's financial statements, they do increase preventable risk to the corporation's financial systems and information.

A key reason for these weaknesses is that FDIC did not always fully implement key information security program activities. For example, it did

not adequately conduct configuration control testing or complete remedial action plans in a timely manner and did not include necessary and key information. Until FDIC fully performs key information security program activities, there is an increased risk that it may not be able to maintain adequate control over its financial systems and information.

We are making 10 recommendations to the Chief Operating Officer to direct the Chief Information Officer (CIO) to address actions to correct access and configuration management control weaknesses and to perform key information security program activities for the NFE and Assessment Information Management System II (AIMS II) systems.

In written comments on a draft of this report, FDIC's Deputy to the Chairman and Chief Financial Officer stated that FDIC has taken action or will take action to improve configuration management and information security. Although FDIC concurred with one and partially concurred with the remaining nine recommendations, the Deputy noted that FDIC has already completed actions to address some of these recommendations and is actively engaged in completing many others. In some instances, FDIC chose to pursue alternative corrective actions. If the corporation effectively implements these alternative actions to reduce risk, it will satisfy the intent of our recommendations.

Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business and is especially important for government agencies, where maintaining the public's trust is essential. While the dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet have enabled corporations such as FDIC to better achieve its mission and provide information to the public, the changes also expose federal networks and systems to various threats. For example, the Federal Bureau of Investigation has identified multiple sources of cyber threats, including foreign nation states engaged in information warfare, domestic criminals, hackers, virus writers, and disgruntled employees working within an organization. According to a May 2005 report by the U.S. Secret Service and the Computer Emergency Response Team (CERT)

Coordination Center,⁷ “insiders pose a substantial threat by virtue of their knowledge of, and access to, employer systems and/or databases.”

These concerns are well-founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology. For example, the number of incidents reported by federal agencies to the United States Computer Emergency Readiness Team (US-CERT) has increased dramatically over the past 3 years, increasing from 3,634 incidents reported in fiscal year 2005 to 13,029 incidents in fiscal year 2007 (about a 259 percent increase).

Without proper safeguards, systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain or manipulate sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

Our previous reports, and those by inspectors general, describe persistent information security weaknesses that place federal agencies at risk of disruption, fraud, or inappropriate disclosure of sensitive information. Accordingly, we have designated information security as a governmentwide high-risk area since 1997,⁸ a designation that remains in force today. Recognizing the importance of securing federal agencies’ information systems, Congress enacted the Federal Information Security Management Act (FISMA) in December 2002⁹ to strengthen the security of information and systems within federal agencies. 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 agency, using a risk-based approach to information security management.

⁷The CERT Coordination Center is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

⁸GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997) and *High-Risk Series: An Update*, [GAO-07-310](#) (Washington, D.C.: January 2007).

⁹FISMA was enacted as title III, E-Government Act of 2002, Pub L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

FDIC Is a Key Protector of Bank and Thrift Depositors

FDIC is an independent agency created by Congress that maintains the stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions, and managing receiverships. Congress created FDIC in 1933¹⁰ in response to the thousands of bank failures that occurred in the 1920s and early 1930s.¹¹ The corporation identifies, monitors, and addresses risks to the deposit insurance funds 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.¹² 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 President signing the Federal Deposit Insurance Reform Act of 2005 into law.¹³ With the congressional approval of the Federal Deposit Insurance Reform Act of 2005, FDIC was required to ensure that approximately 7,400 eligible member institutions received a one-time assessment credit totaling \$4.7 billion.

FDIC insures deposits in excess of \$4 trillion for its 8,571 member institutions. It had a budget of about \$1.1 billion for calendar year 2007 to support its activities in managing the funds. For that year, it processed almost 16.4 million financial transactions.

¹⁰Federal Deposit Insurance Corporation Act, June 16, 1933, Ch. 89, § 8.

¹¹FDIC is considered an independent agency of the federal government and receives no congressional appropriations—it is funded by premiums that banks and thrift institutions pay for deposit insurance coverage and from earnings on investments in U.S. Treasury securities.

¹²Pub. L. No. 101-73, § 211, 103 Stat. 183, 218-22 (Aug. 9, 1989).

¹³Pub. L. No. 109-171, Title II, Subtitle B, § 2102, 120 Stat. 9 (Feb. 8, 2006).

FDIC Reliance on Computer Systems

FDIC relies extensively on computerized systems to support its financial operations and 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 the NFE, a corporate-wide effort focused on implementing an enterprisewide, integrated software system. In addition, the corporation relies on the AIMS II to calculate and collect FDIC deposit insurance premiums and Financing Corporation¹⁴ bond principal and interest amounts from insured financial institutions.¹⁵ FDIC financial systems also process and track financial transactions such as disbursements made to support operations.

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

Two deputies to the Chairman—the Chief Financial Officer and Chief Operating Officer—have information security responsibilities. The Chief Financial Officer has information security responsibilities insofar as he is part of a senior management group that oversees the NFE and AIMS II

¹⁴The Financing Corporation, established by the Competitive Equality Banking Act of 1987, is a mixed-ownership government corporation whose primary purpose was 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.

¹⁵AIMS II has several purposes; the main purpose is the calculation of FDIC insured institutions' insurance assessments and Financing Corporation payments on a quarterly basis. In addition, AIMS II has the functionality to gather the deposit and other data needed to calculate the assessments and Financing Corporation payments; allow FDIC Assessment Operation Section and Assessment Management Section staff to make necessary adjustments/amendments to financial institution demographic and financial data; produce invoices; produce Automated Clearing House files; create assessment entries to post to the NFE-General Ledger; monitor financial institution changes (e.g., new institutions, terminated institutions, mergers, branch sales) and produce management reports.

security team. He is also responsible for the preparation of financial statements and ensures that they are fairly presented and demonstrate discipline and accountability.

In addition, the Chief Operating Officer has information security responsibilities. He supervises the CIO, who is responsible for developing and maintaining a corporate-wide information security program and for developing and maintaining information security policies, procedures, and control techniques that address all applicable requirements. The CIO also serves as the authorizing official with the authority to approve the operation of the information system at an acceptable level of risk to the enterprise. The CIO supervises the Chief Information Security Officer, who is in charge of information security at the corporation. The Chief Information Security Officer serves as the CIO's designated representative responsible for the overall support of the certification and accreditation¹⁶ activities.

FDIC Has Made Significant Progress Mitigating Previously Reported Weaknesses

FDIC has made significant progress in mitigating previously reported information security weaknesses. Specifically, it has corrected or mitigated 16 of the 21 weaknesses that we had previously reported as unresolved at the completion of the 2006 audit (see app. II). For example, FDIC has enhanced physical security controls, instructed personnel to use more secure e-mail methods to protect the integrity of certain accounting data transferred over an internal communication network, updated the NFE security plan to clearly identify all common security controls, developed procedures to report computer security incidents, and updated the NFE contingency plan.

While the corporation has made significant progress in resolving known weaknesses, it has not completed actions to mitigate the remaining five weaknesses. Specifically FDIC has not

- effectively generated NFE audit reports;

¹⁶As a key element of agencies' implementation of FISMA requirements, OMB has continued to emphasize its long-standing policy of requiring a management official to 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.

-
- maintained a complete listing of all NFE configuration items, including application software, data files, software development tools, hardware, and documentation;
 - properly segregated incompatible system-related functions, duties, and capacities for an individual associated with the NFE;
 - effectively implemented or accurately reported the status of its remedial actions; and
 - properly updated the NFE risk assessment.

FDIC stated it has initiated and completed some actions to mitigate the remaining five prior year weaknesses. However, we have not verified that these actions have been completed. Not addressing these actions could leave the corporation's financial data vulnerable to an increased risk of unauthorized access and manipulation.

Appendix II describes the previously reported weaknesses in information security controls that were unresolved at the time of our prior review and the status of the corporation's corrective actions.

Weaknesses Continue to Reduce the Security of Financial Information

Although FDIC has made significant progress improving its information system controls, old and new weaknesses could limit the corporation's ability to effectively protect the confidentiality, integrity, and availability of its financial systems and information. In addition to the five previously reported weaknesses that remain unresolved, newly identified weaknesses in access controls and configuration management controls introduce risk to two key financial systems. A key reason for these weaknesses is that FDIC did not always fully implement key information security program activities. As a result, increased risk exists of unauthorized disclosure or modification of financial information.

Weaknesses in Access Control Warrant Management Attention

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 objective by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computer resources (data, programs, equipment, and facilities), thereby protecting them from unauthorized disclosure, modification, and loss. FDIC developed policies and procedures on access control which, among other things, stated that login ID and password

combinations should not be shared, access to application source code should be restricted unless users have a legitimate business need for access, and passwords should be adequately encrypted.

However, FDIC did not always implement certain access controls, as the following examples show:

- Multiple FDIC users in a production control unit in one division and multiple users in another division share the same NFE logon ID and password. As a result, increased risk exists that individual accountability for authorized, as well as unauthorized system activity could be lost.
- All users of the AIMS II application have full access to the application production code although their job responsibilities do not require such access. As a result, increased risk exists that individuals could circumvent security controls and deliberately or inadvertently read, modify, or delete critical source code.
- One database connection could be compromised because the password is not adequately encrypted with a Federal Information Processing Standards 140-2 compliant algorithm. As a result, increased risk exists that the database could be compromised by unauthorized individuals who could then potentially change, add, or delete information.

Weaknesses in Configuration Management Controls Increased Risk

Our *Federal Information System Controls Audit Manual*¹⁷ states that configuration management 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 consists of four primary areas, each of which should be described in a configuration management plan and implemented according to the plan. The four are as follows:

- *Configuration identification*: procedures for identifying, documenting, and assigning unique identifiers (for example, serial number and name) to requirements, design documents, and the system's hardware and software component parts, generally referred to as configuration items;

¹⁷The current GAO draft *Federal Information System Controls Audit Manual version 2*, the original version Volume I was published in 1999.

-
- *Configuration control*: procedures for evaluating and deciding whether to approve changes to a system's baseline configuration; decision makers such as a Configuration Control Board evaluate proposed changes on the basis of costs, benefits, and risks, and decide whether to permit a change;
 - *Configuration status accounting*: procedures for documenting the status of configuration items as a system evolves; and
 - *Configuration auditing*: procedures for determining traceability between the actual system and the documentation describing it (such as requirements documentation), thereby ensuring that the documentation used to support decision making is complete and correct. Configuration audits are performed when a significant system change is introduced and help to ensure that only authorized changes are being made and that systems are operating securely and as intended.

FDIC has made progress in implementing each of the four configuration management areas. Specifically, for configuration identification, FDIC has documented procedures for identifying and assigning unique identifiers and naming configuration items. For configuration control, it has documented procedures for requesting changes to configuration items, established configuration management plans that document employee roles and responsibilities, developed a Change Control Board that reviews changes to configuration items, and implemented configuration management tools. In addition, for configuration status accounting, FDIC has developed configuration management status accounting reports. Further, for configuration auditing, it has conducted testing and evaluation of releases.

However, FDIC has not executed adequate controls over the configuration management of the NFE and AIMS II information system components. Specifically, it did not adequately (1) maintain a full and complete baseline for system requirements; (2) assign unique identifiers to configuration items; (3) authorize, document, and report all configuration changes; and (4) perform configuration audits. As a result, increased risk exists that functional requirements for these system components were not adequately implemented, managed, or maintained. In addition, increased risk exists that inconsistencies among requirements were not identified, and documents were not correctly associated with the correct releases.

FDIC Did Not Adequately
Maintain a Full and Complete
Requirements Baseline

An entity should maintain current configuration information in a formal configuration baseline that contains the configuration information formally designated at a specific time during a product's or product

component's life. The Software Engineering Institute's Capability Maturity Model® Integration¹⁸ (CMMI) defines a baseline as a set of specifications or work products that has been formally reviewed and agreed on, which thereafter serves as the basis for further development or delivery, and that can be changed only through change control procedures. The NFE configuration management plan states that a baseline is a set of configuration items and their corresponding changes. The plan also states that changes to the requirements baseline should be controlled as part of configuration management throughout the life of the product.

FDIC did not maintain a full and complete requirements baseline for NFE and AIMS II. For example, it could not provide a complete history of all approved requirements and changes to those requirements for NFE. Furthermore, although FDIC officials have stated that RequisitePro¹⁹ is the system of record for requirements, not all requirements for NFE or AIMS II were in RequisitePro. For example, requirements that were documented in the Software Requirement Specification (SRS) and architecture design documents were not included in RequisitePro. As a result, increased risk exists that requirements for these two systems were not adequately implemented, managed, or maintained and that the system may not function as intended.

FDIC Did Not Consistently Assign Unique Identifiers to Configuration Items

Software Engineering Institute's CMMI and the FDIC configuration management plan state that configuration items should have unique identifiers and naming conventions. Identifying items that fall under configuration management control is a key step in the configuration management process. A consistent naming convention for configuration items is important to ensure that requirements are consistently and uniquely identified, verifiable, and traceable. When the requirements have unique identifiers and are managed well, traceability can be established from the source requirement to its lower level requirements and from the lower level requirements back to the source. Such bidirectional traceability through unique identifiers helps determine that all source

¹⁸Software Engineering Institute's CMMI for Development v1.2, August 2006.

¹⁹RequisitePro is a tool that allows organizations to capture, track, manage and analyze different types of requirements.

requirements have been completely addressed and that all lower level requirements can be traced to a valid source.²⁰

FDIC did not consistently assign or use unique identifiers to identify or trace NFE and AIMS II configuration items such as requirements. Specifically, FDIC assigned multiple identifiers for the same requirement and did not always use the assigned identifiers to identify requirements in certain documents. For example, as illustrated in table 1 as follows:

- NFE used “SR numbers” to identify requirements in the implementation report, test plan, test summary, and RequisitePro traceability matrix report but not in the SRS and the design document.
- The NFE requirement numbers on the implementation report and the RequisitePro traceability matrix report were different compared with those identified on the test plan and test summary for the same requirement. For example, the configuration item identifier for change request 4739 was “SR36” on the implementation report and the RequisitePro traceability matrix, but was “SR7” on the test plan and test summary.

²⁰Typical work products associated with this activity include a requirements traceability matrix.

Table 1: NFE Does Not Have Unique Identifiers for the Same Requirement

Document	Change request number	SRS	Design document	Implementation report	Test plan	Test summary	RequisitePro traceability matrix
Requirement identifiers	4739	No SR numbers-only change request numbers	No SR numbers-only change request numbers	SR36	SR7	SR7	SR36
	4757	No SR numbers-only change request numbers	No SR numbers-only change request numbers	SR38	SR3	SR3	SR38
	4782	No SR numbers-only change request numbers	No SR numbers-only change request numbers	SR40,41	SR6	SR6	SR40, 41

Source: GAO analysis of FDIC documentation.

FDIC also did not consistently assign or use unique identifiers to identify or trace AIMS II requirements. For example, the following illustrates this also in table 2:

- AIMS II uses “paragraph numbers” to identify requirements in the SRS, test plan, and RequisitePro traceability matrix report but not in the architecture design document or some instances in the test summary.
- The SRS paragraph number for one particular requirement is described as located at 3.1.1.6; however, the RequisitePro traceability matrix report points to the wrong paragraph number 3.1.1.2 and introduces another identifier “REQS2.”

Table 2: AIMS II Does Not Have Unique Identifiers for the Same Requirement

Document	SRS paragraph number	Architecture design (paragraph number in architecture document)	Test plan (ref to SRS number)	Test summary (ref to SRS number)	RequisitePro traceability matrix (ref to SRS number and RequisitePro number)
Requirement identifiers	3.1.1.6	Component changes: Section 5.2.4, Section 6.3	3.1.1.6	none	3.1.1.2 REQS2
	3.1.1.7	UI changes: Figure 19	3.1.1.7	3.1.1.7	3.1.1.5 REQS5
	3.1.1.8	UI changes: Figure 20	3.1.1.8	3.1.1.8	3.1.1.6 REQS6

Source: GAO analysis of FDIC documentation.

As a result of the lack of consistency in assigning and using unique identifiers for requirements, FDIC had many problems in tracing requirements. For example, our review of the AIMS II release 10.0 SRS, Software Architecture Document, test summary, and RequisitePro reports showed several misalignments in 96 requirements numbers described in the RequisitePro traceability matrix. The following are examples:

- Requirements 3.1.2.7 to 3.1.2.26 are documented in the test summary document but do not appear in the RequisitePro report.
- Requirements 3.1.4.15 through 3.1.4.26 were missing from the SRS and test summary, though they were documented in the RequisitePro report.
- A requirement is also traced to SRS 3.1.1.19 when there is no SRS paragraph 3.1.1.19.

Table 3 illustrates an example of a misaligned AIMS II requirement (3.1.1.8). In this example, “high priority” requirement REQS 8 on the RequisitePro traceability matrix is linked to a requirement in the SRS described as paragraph 3.1.1.8. As can be seen, the requirement has the same number, but the requirement is not the same.

Table 3: AIMS II RequisitePro Requirements on the Traceability Matrix Do Not Match the Software Requirements Specification

Requirement description in AIMS II RequisitePro requirements traceability matrix	AIMS II Requirements traceability matrix stated it is linked to SRS number	SRS with description of the associated number, which does not match the requirement traceability matrix
REQS8: The system shall provide the functionality to apply the one-time credit eligible amount to the institution's FDIC payment. The amount shall be applied as a debit/credit record on its own line on the invoice. The system shall incorporate the business rules to determine the maximum amount that can be applied towards the FDIC payment.	3.1.1.8	3.1.1.8 The Credit Balance Screen shall contain the institution's beginning credit balance, credit amount acquired for the current quarter through acquisitions, credit amount transferred in, credit amount transferred out, total credit amount available for use this quarter, credit amount applied to current quarter assessment, the ending credit balance, and the associated limitations to the credits applied.

Source: GAO analysis of FDIC documentation.

Consequently, traceability cannot be adequately established from the source requirement to its lower level requirements and from the lower level requirements back to the source to ensure that all source requirements have been completely addressed.

FDIC Did Not Adequately Authorize, Document, and Report All Configuration Changes

The Software Engineering Institute's CMMI and the FDIC configuration management plan state that an entity should properly control all configuration changes. This covers a wide range of activities to include the following: a change control board should authorize and approve all configuration changes, change requests should be adequately documented, and status accounting reports should allow users to see baselines, trace requirements throughout the release, and be accurate.

However, FDIC did not adequately authorize, document, and report all configuration changes.

- The FDIC Change Control Board did not authorize and approve all configuration changes for NFE and AIMS II. For example, PeopleSoft access control changes were not made through the Change Control Board.
- Change requests were not adequately documented. For example, implementation date and version number were left out on all change requests for NFE and AIMS II.
- Status accounting reports neither showed baselines, traced requirements throughout the release, nor were accurate. For example, FDIC could not generate a complete requirements baseline report for NFE or AIMS II. In addition, it could not produce configuration management reports of all

PeopleSoft configuration items. Furthermore, traceability reports were manually generated and had many errors.

As a result, increased risk exists that unauthorized changes could be made or introduced to FDIC's systems.

FDIC Did Not Adequately Perform Configuration Audits

Software Engineering Institute's CMMI and the FDIC configuration management plans state that configuration audits should be conducted to verify that the teams are following the configuration management process and to ensure all approved items are built. These audits consist of a physical and functional configuration audit. The physical audit consists of validating and verifying that all items are under configuration management control, configuration items are identified, and team members are following the configuration management process. Another type of configuration audit that must be conducted is the functional configuration audit. A functional configuration audit consists of tracing configuration items from requirements and design to the final delivered release baseline.

FDIC performed limited configuration auditing of NFE and AIMS II. For example, both NFE and AIMS II had developed auditing check lists and made sure independent testing was conducted. However, FDIC did not adequately ensure that configuration audits verified and validated the configuration management process and ensured that all approved items were built. For example, FDIC did not verify and validate in a physical audit that all items are under configuration management control since changes were being made without the Configuration Control Board's approval. In addition, teams were not assigning unique identifiers as required by the configuration management plans. Furthermore, FDIC did not verify and validate in a functional audit that adequate traceability existed since requirements could not be traced backward and forward from design to the final delivered release baseline. As a result, the risk exists that the configuration audits did not adequately verify and validate that functional requirements were adequately implemented, managed, and maintained.

FDIC Has Not Fully Implemented Its Information Security Program

FDIC has made important progress in implementing the corporation's information security program; however, a key reason for these information security weaknesses is that FDIC did not always fully implement key information security program activities. FDIC requires its components to implement information security program activities in accordance with FISMA requirements, Office of Management and Budget (OMB) policies, and applicable National Institute of Standards and Technology (NIST)

guidance. Among other things, FISMA requires agencies to develop, document, and implement

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- plans for providing adequate information security for networks, facilities, and systems;
- security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, 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;
- a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices of the agency;²¹
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

FDIC has taken several actions to implement elements of its information security program. For example, FDIC has

- included nonmajor applications in major systems security plans and developed a new security plan template;

²¹OMB requires agencies to address remedial actions through plan of action and milestones for all programs and systems where an information technology security weakness has been found. The plan lists the weaknesses and shows estimated resource needs, agency head responsible, key milestones and completion dates, and the status of corrective actions.

-
- implemented a risk assessment process that identified possible threats and vulnerabilities to its systems and information, as well as the controls needed to mitigate potential vulnerabilities;
 - implemented a test and evaluation process to assess the effectiveness of information security policies, procedures, and practices;
 - ensured that vulnerabilities identified during its tests and evaluations are addressed in its remedial action plans;
 - established a system for documenting and tracking corrective actions;
 - recognized that NFE users are not physically or logically separated in terms of what they are allowed to access within NFE;
 - implemented an incident handling program, including establishing a team and associated procedures for detecting, responding to, and reporting computer security incidents;
 - developed an incident response policy to review events related to data loss, disclose, inappropriate access and loss of equipment in the Division of Finance to determine whether the events are computer security incidents; and
 - developed the corporation's business continuity of operations, updated the contingency plans and business impact analyses, and assessed the effectiveness of the plans through testing at a disaster recovery site.

However, FDIC did not always fully implement key information security program activities for NFE and AIMS II. For example, it did not adequately conduct configuration control testing or complete remedial action plans in a timely manner to include key information. Until FDIC fully performs key information security program activities, its risk is increased because it may not be able to maintain adequate control over its financial systems and information.

Although Controls Were Tested and Evaluated, Tests Were Not Always Adequate

A key element of an information security program is testing and evaluating system configuration controls to ensure that they are appropriate, effective, and comply with policies. According to NIST, the organization should (1) develop, document, and maintain a current baseline configuration of the information system and update the baseline configuration of the information system and (2) assess the degree of

consistency between system documentation and its implementation in security tests, to include tests of configuration management controls.

FDIC did not adequately test NFE configuration management controls. We found that the depth of FDIC's system testing and evaluation for configuration management controls were insufficient since we identified vulnerabilities in the configuration management process during our testing that FDIC did not. Specifically, the NFE system test and evaluation report stated that FDIC developed, documented, and maintained a current baseline configuration; however, as we have previously stated in the report, we found that FDIC did not maintain a full and complete requirements baseline for NFE. In addition, the NFE system test and evaluation stated that FDIC authorizes and controls changes to the information system; however, as we have previously stated in the report, we found that some configuration changes were not being authorized and controlled by the Configuration Control Board. Furthermore, the NFE system test and evaluation stated that configuration items were uniquely identified and stored in configuration management libraries, yet we found FDIC had problems assigning unique identifiers to configuration items for NFE. As a result, without adequate tests and evaluations of configuration management controls, FDIC has limited assurance that the nature of configuration controls are being effectively tested and reported.

The Remedial Action Plan Was Not Completed in A Timely Manner and Did Not Include Necessary and Key Information

A remedial action plan is a key component described in FISMA. Such a plan assists agencies in identifying, assessing, prioritizing, and monitoring progress in correcting security weaknesses that are found in information systems. In its annual FISMA guidance to agencies, OMB requires that agencies' remedial action plans (also known as plan of action and milestones) include the resources necessary to correct an identified weakness. According to FDIC policy, the agency should document weaknesses found during security assessments. The policy further requires that FDIC track the status of resolution of all weaknesses and verify that each weakness is corrected.

The NFE remedial action plan was not completed in a timely manner and did not include necessary and key information. FDIC performed a system test and evaluation of NFE in November 2007 and developed a plan of action and milestones to correct any identified weaknesses. However, the plan of action and milestones report did not contain necessary and key information such as the contact that will be responsible for the corrective action, when the action will be closed, and status of the action. For example, the plan of action and milestones document included problems with the PeopleSoft security roles and functions; however, it did not state

how FDIC would address these issues. FDIC officials stated that they were in the process of completing the plan of action and milestones with the required information but had not established a milestone date for doing so. Until the plan contains necessary and key information, FDIC's assurance is reduced that the proper resources will be applied to known vulnerabilities or that those vulnerabilities will be properly mitigated.

Conclusions

FDIC has made significant progress in correcting previously reported weaknesses and has taken steps to improve information security. Although five weaknesses from prior reports remain unresolved and new control weaknesses related to access control and configuration management were identified, the remaining unresolved weaknesses previously reported and the newly identified weaknesses did not pose significant risk of material misstatements in the corporation's financial statements for calendar year 2007. However, these weaknesses increase preventable risk to the corporation's financial and sensitive systems and information and warrant management's immediate attention.

A key reason for these weaknesses is that FDIC did not always fully implement key information security program activities. Continued management commitment to mitigating known information security weaknesses in access controls and configuration management and fully implementing its information security program will be essential to ensure that the corporation's financial information will be adequately protected from unauthorized disclosure, modification, or destruction, and its management decisions may be based on reliable and accurate information.

Recommendations for Executive Action

In order to sustain progress to its program, we recommend that the Chief Operating Officer direct the CIO to take the following 10 actions:

Improve access controls by ensuring that

- NFE users do not share login ID and password accounts;
- AIMS II users do not have full access to application source code, unless they have a legitimate business need; and
- the database connection is adequately encrypted with passwords that comply with FIPS 140-2.

Improve NFE and AIMS II configuration management by ensuring that

- full and complete requirement baselines are developed and implemented;
- configuration items have unique identifiers;
- configuration changes are properly authorized, documented, and reported;
- physical configuration audits verify and validate that all items are under configuration management control, all changes made are approved by the configuration control board, and that teams are assigning unique identifiers to configuration items; and
- functional configuration audits verify and validate that requirements have bidirectional traceability and can be traced from various documents.

Improve the security management of NFE and AIMS II by ensuring that users

- adequately test configuration management controls as part of the system test and evaluation process and
- develop in a timely manner a detailed plan of action and milestones to include who will be responsible for the corrective action, when the action will be closed, and status of the action for NFE.

Agency Comments and Our Evaluation

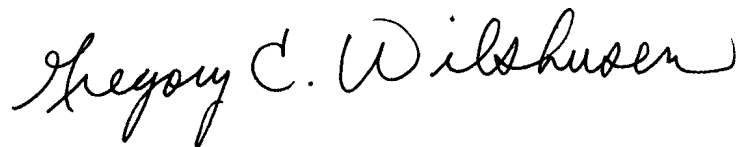
We received written comments on a draft of this report from FDIC's Deputy to the Chairman and Chief Financial Officer (which are reprinted in app. III). The Deputy stated that FDIC concurred with one recommendation and partially concurred with the remaining nine. He added that, in general, FDIC found the issues to be more limited than presented in the draft report, yet FDIC has taken action or will take action to improve configuration management and information security. We believe that the issues we presented in the report are accurately presented and can increase the risk of unauthorized disclosure, modification, or destruction of the corporation's financial information and that management decisions may be based on unreliable or inaccurate information.

Regarding the nine recommendations to which FDIC partially concurred, the Deputy stated that the corporation has developed or implemented plans to adequately address the underlying risks that prompted these nine

recommendations, and in some instances, pursued alternative corrective actions. If the corporation effectively implements the alternative corrective actions to reduce risk, it will satisfy the intent of the recommendations. In addition, the Deputy provided technical comments, which we incorporated into the report as appropriate.

We are sending copies of this report to the Chairman and Ranking Member of the Senate Committee on Banking, Housing, and Urban Affairs; the Chairman and Ranking Member of the House Committee on Financial Services; members of the FDIC Audit Committee; officials in FDIC's divisions of information resources management, administration, finance; the FDIC inspector general; and other interested parties. We also will make copies available to others upon request. 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 Offices 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 IV.



Gregory C. Wilshusen
Director, Information Security Issues



Dr. Nabajyoti Barkakati
Director, Center for Technology and Engineering

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to assess (1) the progress the Federal Deposit Insurance Corporation (FDIC) has made in mitigating previously reported information security weaknesses and (2) the effectiveness of FDIC's controls in protecting the confidentiality, integrity, and availability of its financial systems and information. An integral part of our objectives was to support the opinion on internal control in GAO's 2007 financial statement audit by assessing the controls over systems that support financial management and the generation of the FDIC funds' financial statements.

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.

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, enterprise database applications, and network infrastructure associated with the New Financial Environment (NFE) release 1.43 and the Assessment Information Management System II (AIMS II) release 10.0 applications.¹

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.

¹AIMS II release 10.0 involved the implementation of requirements associated with the implementation of the deposit insurance reform legislation in the Deficit Reduction Act of 2005, Pub. L. No. 109-171, enacted February 8, 2006. Among the new requirements based on the legislation was the introduction of credits and dividends. FDIC was required to issue credits to some insured financial institutions, based on their status and contributions to the insurance fund as of specific dates. Such credits were based on the assessment base of the eligible institution as of December 31, 1996. Dividends were then to be paid to qualifying institutions based on limits for the Deposit Insurance Fund. A requirement of the Federal Deposit Insurance Reform Act of 2005 was to merge the Bank Insurance Fund and Savings Association Insurance Fund into one fund, the Deposit Insurance Fund.

Using 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 was being encrypted;
- testing and observing physical access controls to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft;
- evaluated 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;
- examining access responsibilities to determine whether incompatible functions were segregated among different individuals; and,
- observing end-user activity pertaining to the process of preparing FDIC financial statements.

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 two 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 received training commensurate with those responsibilities;

- analyzing configuration management plans and procedures to determine if configurations are being managed appropriately;
- analyzing security testing and evaluation results for two 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 the FDIC's security testing and evaluations; and
- examining contingency plans for two 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. We conducted this audit work from October 2007 to May 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Status of Previously Reported Weaknesses

This appendix describes the status of the information security weaknesses we reported last year. It also includes the status of weaknesses from previous reports that were not fully implemented during the time of our last review.

Control areas	Year initially reported	Action completed	Action in progress
Access controls			
<i>Access rights and permissions</i>			
1. FDIC did not effectively limit network access to sensitive personally identifiable and business proprietary information.	2006	X	
<i>Audit and monitoring of security-related events</i>			
2. FDIC did not effectively generate NFE audit reports or review them.	2006		X
<i>Cryptography</i>			
3. FDIC did not use secure e-mail methods to protect the integrity of certain accounting data transferred over an internal communication network.	2007	X	
<i>Physical security</i>			
4. FDIC did not adequately control physical access to the Virginia Square computer processing facility.	2006	X	
5. FDIC did not apply physical security controls for some instances. For example, an unauthorized visitor was able to enter a key FDIC facility without providing proof of identity, signing a visitor log, obtaining a visitor's badge, or being escorted.	2007	X	
6. FDIC did not apply physical security controls for some instances. For example, a workstation that had access to a payroll system was located in an unsecured office.	2007	X	
Configuration management (formerly application change control)			
7. Procedures have not been consistently followed for authorizing, documenting, and reviewing all application software changes.	2005	X	
8. FDIC did not consistently implement configuration management controls for NFE. Specifically, the corporation did not develop and maintain a complete listing of all configuration items and a baseline configuration for NFE, including application software, data files, software development tools, hardware, and documentation.	2007		X
9. FDIC did not ensure that all significant system changes, such as parameter changes, go through a change control process.	2007	X	
10. FDIC did not apply comprehensive patches to system software in a timely manner.	2007	X	
11. FDIC did not review status accounting reports, or perform complete functional and physical configuration audits.	2007	X	
12. FDIC did not update or control documents to reflect the current state of the environment and to ensure consistency with related documents.	2007	X	
Segregation of duties			
13. FDIC did not properly segregate incompatible system-related functions, duties, and capacities for an individual associated with NFE.	2006		X

Appendix II: Status of Previously Reported Weaknesses

Control areas	Year initially reported	Action completed	Action in progress
Security management (formerly information security program)			
14. FDIC has documented various policies for establishing effective information security controls; however, the corporation has not consistently implemented them.	2006	X	
15. FDIC did not integrate the security plans or requirements for certain nonmajor applications into the security plan for the general support system. Two of FDIC's nonmajor applications, the corporation's human resources and time and attendance systems, are not included in FDIC general support systems security plans.	2006	X	
16. FDIC did not effectively implement or accurately report the status of its remedial actions.	2006		X
17. FDIC did not update its business impact analysis to reflect the significant changes resulting from the implementation of NFE.	2006	X	
18. The risk assessment for FDIC's NFE was not properly updated.	2007		X
19. The corporation did not update the system security plan for NFE.	2007	X	
20. The corporation did not always review events occurring in NFE to determine whether the events were computer security incidents or not.	2007	X	
21. FDIC's NFE contingency plan was not updated to reflect the new disaster recovery site. In addition, the plan identified servers that were not in use.	2007	X	

Source: GAO.

Appendix III: 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

May 14, 2008

Mr. Gregory C. Wilshusen
Director, Information Security Issues
Dr. Nabajyoti Barkakati
Acting Chief Technologist
Government Accountability Office
Washington, D.C. 20548

Re: FDIC Management Response to the GAO 2007 Audit of FDIC's Information Security Program

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: FDIC Sustains Progress but Needs to Improve Configuration Management of Key Financial Systems, GAO-08-564. The report presents GAO's assessment of the progress the Federal Deposit Insurance Corporation (FDIC) has made in correcting or mitigating remaining information system control weaknesses reported as unresolved at the time of the GAO's prior review in 2006, as well as outlining GAO's findings with respect to the effectiveness of the Corporation's information system controls for protecting the confidentiality, integrity, and availability of its information and information systems during 2007.

We are pleased to accept GAO's acknowledgement of the significant progress FDIC has made in correcting previously reported weaknesses and improving its information security controls. We are also pleased to have GAO acknowledge that, although the weaknesses identified warrant FDIC management's attention, they do not pose a significant risk to the integrity of the financial statements of either the Deposit Insurance Fund (DIF) or the FSLIC Resolution Fund (FRF). Further, we appreciate the work of the GAO and recognize the benefit of a number of the recommendations made as part of this year's audit. The FDIC has, in fact, already completed actions to address some of those recommendations and is actively engaged in completing many others.

The GAO's report contains ten new recommendations to assist FDIC in further strengthening its information security program. FDIC has reviewed the recommendations along with the accompanying statements of condition on which the recommendations are based. In general, FDIC found the issues to be more limited than presented in the draft report; however, FDIC has taken action or will take action to improve configuration management and information security. At this time the FDIC concurs with one of the findings and recommendations and partially concurs with the remaining nine. In instances where FDIC did not fully concur with specific GAO findings and recommendations, FDIC has developed or implemented plans to adequately address the underlying risks that prompted the recommendations. In some instances,

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

Mr. G. Wilshusen and Dr. N. Barkakati

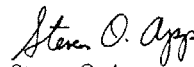
May 14, 2008

we chose to pursue alternative corrective actions. The detailed responses to these ten new recommendations are provided in Attachment 1. Appendix II of the GAO's report cites five weaknesses that were identified in the previous IT security audit and that GAO concludes remain unresolved. Our responses to these five prior year weaknesses are provided in Attachment 2. For all but two weaknesses identified in GAO's report, corrective action has already been or will be completed by December 31, 2008. Corrective action for the remaining two, which are generally low risk issues, will involve multi-year efforts to ensure a complete solution.

Once again, we thank you for your past contributions and your work on this year's audit. We look forward to our dialogue with the GAO as we continue to enhance our information security program and to discussing mutually beneficial process improvements for the upcoming year.

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: John Bovenzi
Michael Bartell
Bret Edwards
James H. Angel, Jr.
Audit Committee

Appendix IV: 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, William F. Wadsworth (Assistant Director), Angela M. Bell, Neil J. Doherty, Patrick R. Dugan, Mickie E. Gray, David B. Hayes, Tammi L. Nguyen, Eugene E. Stevens IV, Amos A. Tevelow, and Jayne L. Wilson 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, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

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