United States Government Accountability Office

GAO

Report to the Board of Directors, Federal Deposit Insurance Corporation

August 2006

INFORMATION SECURITY

Federal Deposit Insurance Corporation Needs to Improve Its Program

GAO-06-620

August 2006

INFORMATION SECURITY

Federal Deposit Insurance Corporation Needs to Improve Its Program

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-620, a report to the Board of Directors, 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. The corporation relies extensively on computerized systems to support and carry out its financial and mission-related operations.

As part of the audit of the calendar year 2005 financial statements, GAO assessed (1) the progress FDIC has made in correcting or mitigating information security weaknesses previously reported and (2) the effectiveness of the corporation's information system controls to protect the confidentiality, integrity, and availability of its key financial information and information systems.

What GAO Recommends

GAO recommends that the FDIC Chairman fully implement key elements of its agencywide information security program. In providing written comments on a draft of this report, FDIC's Deputy to the Chairman and Chief Financial Officer stated that FDIC concurred with one of GAO's recommendations, partially concurred with three, and did not concur with one. FDIC also disagreed with GAO's assessment that its information system control weaknesses were sufficient to constitute a reportable condition.

www.gao.gov/cgi-bin/getrpt?GAO-06-620.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

FDIC has made progress in correcting previously reported weaknesses. Specifically, the corporation has corrected or mitigated 18 of the 24 weaknesses that GAO previously reported as unresolved at the time of the last review. Among actions FDIC has taken are developing and implementing procedures to comply with its computer file naming convention standards and developing and implementing automated procedures for limiting access to sensitive information.

Nevertheless, FDIC has not consistently implemented information security controls to properly protect the confidentiality, integrity, and availability of its financial and sensitive information and information systems. In addition to the remaining six previously reported weaknesses for which FDIC has not completed corrective actions, GAO identified 20 new information security weaknesses. Most identified weaknesses pertain to access controls over (1) user accounts and passwords; (2) access rights and permissions; (3) network services; (4) configuration assurance; (5) audit and monitoring of security-related events; and (6) physical security that are to prevent, limit, or detect access to its critical financial and sensitive systems and information. In addition, weaknesses exist in other information security controls relating to segregation of duties and application change controls.

A key reason for these weaknesses is that FDIC has not fully implemented elements of its information security program. For example, it has not consistently implemented its security-related policies, addressed security plans for certain applications, provided specialized training to individuals with significant security responsibilities, implemented remedial action plans for resolving known weaknesses, and updated or tested continuity plans in light of its implementation of the new financial environment. As a result, financial and sensitive information are at increased risk of unauthorized access, modification, and/or disclosure, possibly without detection. Because of this, GAO reported information system control weaknesses to be a reportable condition in 2005.

Contents

Abbreviations

FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Management Act
FSLIC	Federal Savings and Loan Insurance Corporation
NFE	New Financial Environment
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

August 31, 2006

To the Board of Directors
Federal Deposit Insurance Corporation

The Federal Deposit Insurance Corporation (FDIC) has a demanding responsibility enforcing banking laws, regulating banking institutions, and protecting depositors. In enforcing banking laws, it plays an important role in maintaining public confidence in the nation's financial system. The corporation relies extensively on computerized systems to support and carry out its financial and mission-related operations.

Effective information security controls[1] affect the integrity, confidentiality, and availability of sensitive information—such as personnel and regulatory information—maintained by FDIC. These controls are essential to ensure that financial information is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

As part of our audit of the calendar year 2005 financial statements for FDIC's Bank Insurance Fund, the Savings Association Insurance Fund, and the Federal Savings and Loan Insurance Corporation (FSLIC) Resolution Fund,[2] we assessed (1) the progress FDIC has made in correcting or mitigating remaining information system control weaknesses reported as unresolved at the time of our prior review in 2004[3] and (2) the effectiveness of the corporation's information system controls for protecting the confidentiality, integrity, and availability of its information and information systems.

[1]Information system general controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. These controls include security 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.

[2]GAO, *Financial Audit: Federal Deposit Insurance Corporation Funds' 2005 and 2004 Financial Statements*, GAO-06-146 (Washington, D.C.: Mar. 2, 2006).

[3]GAO, *Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress*, GAO-05-486 (Washington, D.C.: May 19, 2005) and *Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress* (Limited Official Use Only), GAO-05-487SU (Washington, D.C.: May 19, 2005).

We performed our review at FDIC headquarters in Washington, D.C., and its computer facility in Arlington, Virginia, from September 2005 through February 2006. Our review was performed in accordance with generally accepted government auditing standards.

Results in Brief

FDIC has made progress in correcting previously reported weaknesses. Specifically, the corporation has corrected or mitigated 18 of the 24 weaknesses that we previously reported as unresolved at the time of our last review. Among actions FDIC has taken include developing and implementing procedures to comply with its computer file naming convention standards and developing and implementing automated procedures for limiting access to sensitive information.

Nevertheless, the corporation has not consistently implemented information security controls to properly protect the confidentiality, integrity, and availability of its financial and sensitive information and information systems. In addition to the six previously reported weaknesses that remain uncorrected, other newly identified information security weaknesses exist. For example, FDIC did not consistently implement controls intended to prevent, limit, or detect access to its critical financial and sensitive systems and information. Weaknesses in access controls exist related to (1) user accounts and passwords, (2) access rights and permissions, (3) network services, (4) configuration assurance, (5) audit and monitoring of security-related events, and (6) physical security. In addition, weaknesses existed in other information security controls designed to prevent assigning incompatible duties among multiple individuals or groups and prevent unauthorized changes to application programs. A key reason for these weaknesses is that FDIC had not fully implemented components of its information security program. The collective severity of these weaknesses was such that we reported information system control weaknesses to be a reportable condition in our report on the FDIC funds' 2005 financial statements[4] since it increased the risk of unauthorized modification and disclosure of critical FDIC financial and sensitive personnel information, disruption of critical operations, and loss of assets.

[4]GAO-06-146.

We are recommending that the FDIC Chairman take actions to fully implement key components of the corporation's information security program.

We are making additional recommendations in a separate report designated for "Limited Official Use Only."[5] These recommendations address actions needed to correct specific information security weaknesses related to access controls and other information systems controls.

In providing written comments on a draft of this report (which are reprinted in app. I), FDIC's Deputy to the Chairman and Chief Financial Officer stated that FDIC concurred with one of our recommendations, partially concurred with three, and did not concur with one. FDIC also disagreed with our assessment that its information system control weaknesses were sufficient to constitute a reportable condition.

The Deputy stated that FDIC agreed with our recommendation that it include security plans or requirements for nonmajor applications into the plans for general support systems. However, FDIC questioned the need for it to assess the security plans for its payroll service provider because the provider is federally certified and audited, and therefore such effort on its part would be duplicative. We agree with the FDIC position and have revised the report accordingly.

For the three recommendations for which FDIC's concurrence was partial, the Deputy generally agreed with the thrust of the recommendations but took issue with details of our analysis or described why the corporation was already compliant. With regard to one recommendation, FDIC did not agree with aspects of our assessment of compliance with information security policies and procedures, providing two examples of factors mitigating the weaknesses we described. Although we agree that FDIC has taken steps that may mitigate these weaknesses, we believe that the weaknesses continue to increase the security risks that the corporation faces. With regard to two recommendations regarding security training and continuity of operations planning, the Deputy stated that FDIC believed that it was already in compliance with these recommendations because of actions taken since the completion of our field work. Although we have not

[5]GAO, *Information Security: Federal Deposit Insurance Corporation Needs to Improve Its Program* (Limited Official Use Only), GAO-06-619SU (Washington, D.C.: Aug. 31, 2006).

evaluated these actions, if they have been implemented appropriately FDIC will have satisfied our recommendations.

FDIC did not concur with our recommendation that it report weaknesses as closed in remedial action plans only when corrective actions are taken. According to the Deputy, FDIC disagreed with the assessment on which this recommendation was based; that is, that FDIC did not effectively implement or accurately report the status of remedial actions. According to FDIC, our finding was based on a single instance and was not valid for the program that was in place through most of 2005. However, we disagree with FDIC's characterization that our observation was based on a single instance. FDIC had reported 38 control weaknesses associated with its New Financial Environment (FDIC's modernized financial system) as closed before it had tested or validated them. Similar instances of weaknesses closed without test or validation occurred in a remediation plan resulting from a second security test and evaluation of this system. In addition, we do not agree that our finding was not valid for the program that was in place through most of 2005, because the remediation plans on which it is based were dated November and December 2005 and were still active at that time. Thus, we continue to believe that FDIC implemented a flawed process which could mislead management to think that risks had been lowered when in fact they had not.

Finally, FDIC disagreed with our assessment that its information system control weaknesses were sufficient to be a reportable condition for the FDIC funds' 2005 financial statements. In the corporation's view, the risk impact and magnitude of the vulnerability were not sufficient to earn this assessment; FDIC is nonetheless pursuing completion of actions to address information security weaknesses. We continue to believe that the problems identified in this report amounted to a reportable condition because they increased the risk of unauthorized modification and disclosure of critical FDIC financial information and sensitive personnel information, disruption of critical operations, and loss of assets.

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. It is especially important for government agencies where maintaining the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. Without proper safeguards, systems

are unprotected from individuals and groups with malicious intent to intrude and use the access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. 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, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks to come.

Computer-supported federal operations are likewise at risk. Our previous reports, and those of agency inspectors general, describe persistent information security weaknesses that place a variety of federal operations at risk of disruption, fraud, and inappropriate disclosure. We have designated information security as a governmentwide high-risk area since 1997[6]—a designation that remains today.[7]

Recognizing the importance of securing the information systems of federal agencies, Congress enacted the Federal Information Security Management Act of 2002 (FISMA) to strengthen the security of information and systems within federal agencies.[8] 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.

FDIC Is a Key Protector of Bank and Thrift Depositors

Congress created FDIC in 1933[9] to restore and maintain public confidence in the nation's banking system. The *Financial Institutions Reform, Recovery, and Enforcement Act of 1989* sought to reform, recapitalize, and consolidate the federal deposit insurance system.[10] The act created the Bank Insurance Fund and the Savings Association Insurance Fund, both of

[6]GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997).

[7]GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

[8]FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347 (2002).

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

[10]Pub. L. No. 101-73 (1989).

which are responsible for protecting insured bank and thrift depositors.[11] It also abolished the FSLIC and created the FSLIC Resolution Fund to complete the affairs of the former FSLIC and liquidate the assets and liabilities transferred from the former Resolution Trust Corporation. Further, the act designated the corporation as the administrator of these funds. As part of this function, it has an examination and supervision program to monitor the safety of deposits held in member institutions.

FDIC insures deposits in excess of $7 trillion for about 8,800 institutions. Together, the funds administered by FDIC have about $53 billion in assets. FDIC had a budget of about $1.1 billion for calendar year 2005 to support its activities in managing the funds. For that year, it processed almost 21 million financial transactions.

The corporation relies extensively on computerized systems to support its financial operations and store the sensitive information it collects. Its local and wide area networks interconnect these systems. To support its financial management functions, the corporation relies on several financial systems to process and track financial transactions that include premiums paid by its member institutions and disbursements made to support operations. In addition, FDIC uses other systems that maintain personnel information for its employees, examination data for financial institutions, and legal information on closed institutions. At the time of our review, there were about 6,100 users on its systems.

In our report on the results of our audit of the FDIC funds' financial statements for 2003 and 2004,[12] we noted that FDIC's implementation of a new financial system would significantly change its information systems environment and the related information systems controls necessary for their effective operation and that, consequently, continued commitment to an effective information security program would be essential to ensure that the corporation's financial and sensitive information would be adequately protected in the new environment.

[11]On February 8, 2006, the *Federal Deposit Insurance Reform Act of 2005 was* signed into law. Among its provisions, the act calls for the merger of the Bank Insurance Fund and the Savings Association Insurance Fund into a single Deposit Insurance Fund no later than the first day of the first calendar quarter that begins after the 90-day period beginning on the date of enactment, which was July 1, 2006. The Bank Insurance Fund and the Savings Association Insurance Fund were merged on March 31, 2006.

[12]GAO, *Financial Audit: Federal Deposit Insurance Corporation Funds' 2004 and 2003 Financial Statements*, GAO-05-281 (Washington, D.C.: Feb. 11, 2005).

To support the corporation's financial management functions in 2005, FDIC implemented its new financial system in May 2005. The new financial system is composed of 26 separate applications that either replaced or modified previous applications to support the New Financial Environment (NFE). In addition to changing financial systems, FDIC has undergone organizational changes in the last year that include the reorganization of the Division of Information Technology. This division oversees the development and operation of the corporation's computer systems and software. It maintains the corporation's communications network and provides the expertise necessary for developing new information management systems needed by the FDIC's bank examiners, researchers, legal case managers, and finance officers.

According to 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 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 agency's Chief Information Officer the authority to ensure compliance with the requirements imposed on the agency under FISMA. The corporation's Chief Information Officer is responsible for developing and maintaining a departmentwide information security program and for developing and maintaining information security policies, procedures, and control techniques that address all applicable requirements.

Objectives, Scope, and Methodology

The objectives of our review were to assess (1) the progress FDIC has made in correcting or mitigating remaining information system control weaknesses reported as unresolved at the time of our prior review in 2004[13] and (2) the effectiveness of the corporation's information system controls for protecting the confidentiality, integrity, and availability of computerized data. An integral part of our objectives was to support the 2005 financial audit by assessing, as of December 31, 2005, the degree of security and controls over systems that support the generation of the FDIC funds' financial statements.

[13]GAO-05-486 and GAO-05-487SU.

Our scope and methodology was based on our *Federal Information System Controls Audit Manual*,[14] which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized data. Focusing on FDIC's financial systems and associated infrastructure, we evaluated the effectiveness of information security controls that are intended to

- prevent, limit, and detect access to computer resources (data, programs, and systems), thereby protecting these resources against unauthorized disclosure, modification, and use;
- provide physical protection of computer facilities and resources from unauthorized use, espionage, sabotage, damage, and theft;
- prevent the exploitation of vulnerabilities;
- prevent the introduction of unauthorized changes to application or system software; and
- ensure that work responsibilities for computer functions are segregated so that one individual does not perform or control all key aspects of computer-related operations and, thereby, have the ability to conduct unauthorized actions or gain unauthorized access to assets or records without detection.

In addition, we evaluated aspects of FDIC's information security program. This program includes assessing risk; developing and implementing policies, procedures, and security plans; promoting security awareness and providing specialized training for those with significant security responsibilities; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; detecting, reporting, and responding to security incidents; and ensuring the continuity of operations.

To evaluate FDIC's information security controls and program, we identified and examined pertinent FDIC security policies, procedures, guidance, security plans, and relevant reports provided during field work. In addition, we conducted tests and observations of controls in operation

[14]GAO, *Federal Information System Controls Audit Manual*, *Volume I-Financial Statements Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

and reviewed corrective actions taken by the corporation to address vulnerabilities identified during our previous review.[15] We also discussed with key security representatives, system administrators, and management officials whether information system controls were in place, adequately designed, and operating effectively.

We performed our review at FDIC headquarters in Washington, D.C., and its computer facility in Arlington, Virginia, from September 2005 through February 2006. Our review was performed in accordance with generally accepted government auditing standards.

FDIC Has Made Progress Correcting Previously Reported Weaknesses

FDIC has taken steps to address security control weaknesses. The corporation has corrected or mitigated 18 of the 24 weaknesses that we previously reported as unresolved. For example, the corporation has

- established and implemented procedures to ensure that dataset naming conventions comply with FDIC standards;
- developed and implemented automated procedures to ensure that access to sensitive production data is limited; and
- documented the appropriate controls of system interconnections, sharing information between applications, and rules concerning the behavior of users within each application between the Department of Agriculture's National Finance Center and FDIC.

While the corporation has made progress in strengthening its information security controls, it is still in the process of completing actions to correct or mitigate the remaining six previously reported weaknesses. These weaknesses include not adequately securing personal firewall settings on laptop computers, using live data for testing, and not ensuring that only authorized application software changes are implemented. Failure to resolve these issues could leave the corporation's sensitive data vulnerable to unauthorized access and manipulation.

[15] GAO-05-486 and GAO-05-487SU.

Control Weaknesses Place Financial and Sensitive Data at Risk

FDIC has not effectively implemented information security controls to properly protect the confidentiality, integrity, and availability of its financial and sensitive information and information systems. In addition to the 6 previously reported weaknesses that remain uncorrected, we identified 20 new information security weaknesses during this review. Most of the identified weaknesses pertain to access controls. A primary reason for these weaknesses is that FDIC has not yet fully implemented its information security program. As a result, weaknesses in controls over its financial and sensitive data increase the risk of unauthorized disclosure, modification, or loss of data. Because of these heightened risks, we concluded that the weaknesses we identified constituted a reportable condition with respect to FDIC's information systems security for 2005.

Access Controls Were Not Always Effective

Protecting the resources that support critical operations from unauthorized access is a basic management objective for any organization. Organizations accomplish this objective by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, and information. Access controls include (1) user accounts and passwords, (2) access rights and permissions, (3) network services, (4) configuration assurance, (5) audit and monitoring of security-related events, and (6) physical security. Inadequate access controls diminish the reliability of computerized information, and they increase the risk of unauthorized disclosure, modification, and loss of sensitive information and of disruption of service.

User Accounts and Passwords

A computer system must be able to identify and differentiate among users so that activities on the system can be linked to specific individuals. When an organization assigns unique user accounts to specific users, the system distinguishes one user from another—a process called identification. The system must also establish the validity of a user's claimed identity through some means of authentication, such as a password, that is known only to its owner. The combination of identification and authentication, such as user account/password combinations, provides the basis for establishing individual accountability and for controlling access to the system. Accordingly, agencies implement procedures to, among other things, (1) modify vendor-supplied default authenticators during information system installation and (2) create, use, and remove user accounts.

FDIC has not adequately controlled user accounts and passwords to ensure that only authorized individuals are granted access to its systems and data.

For example, the corporation did not change vendor-supplied administrator accounts and passwords or remove inactive user accounts. In 2002 and 2003, we reported the existence of these weaknesses and in 2004 reported that FDIC had corrected them.[16] The reemergence of these weaknesses demonstrates that FDIC had not implemented disciplined processes for ensuring that such issues do not recur. As a result, there is increased risk that unauthorized users could gain valid user identification and password combinations to claim a user identity and then use that identity to gain access to corporation systems.

Access Rights and Permissions

A basic underlying principle for secure computer systems and data is the concept of least privilege, which means that users are granted only those access rights and permissions needed to perform their official duties. User rights are allowable actions that can be assigned to users or groups. File and directory permissions are rules associated with a particular file or directory; they regulate which users can access the file or directory and in what manner. Organizations establish access rights and permissions to restrict legitimate users' access to only those programs and files that they need to do their work. Assignment of rights and permissions must be carefully considered to avoid giving users unnecessary access to sensitive files and directories, especially to protect personal information maintained in systems of records. Further, the Privacy Act of 1974[17] requires federal agencies to limit the collection, disclosure, and use of personal information maintained in systems of records and to establish reasonable safeguards over those records.

FDIC sometimes permitted excessive access to the computer systems that support its critical financial and regulatory operations. For example, the corporation inadvertently granted excessive access to insurance and research data that could result in the inappropriate modification or deletion of this data. FDIC also permitted each user on its networks to have access to sensitive Privacy Act-protected information including names, addresses, and Social Security numbers of individuals corresponding with

[16]GAO, *Information Security: Information System Controls at the Federal Deposit Insurance Corporation* (Limited Official Use Only), GAO-04-629 (Washington, D.C.: May 28, 2004); GAO, *FDIC Information Security: Progress Made but Existing Weaknesses Place Data at Risk* (Limited Official Use Only), GAO-03-629 (Washington, D.C.: June 18, 2003); and GAO, *FDIC Information Security: Improvements Made but Weaknesses Remain* (Limited Official Use Only), GAO-02-688 (Washington, D.C.: July 15, 2002).

[17]5 U.S.C. § 552a.

the corporation. The FDIC Office of Inspector General recently reported on the misuse of sensitive employee information, including Social Security numbers, resulting in fraud.[18] We recently testified that, once a Social Security number is obtained fraudulently, it can then be used to create a false identity for financial misuse, assume another individual's identity, or to fraudulently obtain credit.[19] As a result, there is increased risk that FDIC's sensitive data and personally identifiable information may be compromised.

Network Services

Networks are a series of interconnected devices and software that allow individuals to share data and computer programs. Because sensitive programs and data are stored on network servers or transmitted along networks, effectively securing networks is essential to protecting computing resources and data from unauthorized access, manipulation, and use. Remote access controls should restrict access to networks from sources external to the network. Controls should also limit the use of systems from sources internal to the network to authorized users for authorized purposes. Organizations secure their networks, in part, by installing and configuring network devices that permit authorized network service requests and deny unauthorized requests and by limiting the services that are available on the network.

FDIC did not sufficiently control certain network services. It did not securely configure Internet-accessible remote access services to its network resources. For example, the remote access configuration did not support the government advanced encryption standard and certificates used for authentication did not require passwords and could be stored as insecure files. FDIC permitted the use of unencrypted network protocols on its UNIX systems, thereby increasing the risk of unauthorized disclosure of sensitive information, including valid user passwords. As a result, increased risk exists that a malicious user could gain unauthorized access to network resources.

Configuration Assurance

To protect an organization's information, it is important to ensure that only authorized configurations are placed in operation. This process, known as

[18]FDIC OIG, *FDIC Safeguards Over Personal Employee Information* (Washington, D.C.: Jan. 6, 2006).

[19]GAO, *Social Security Numbers: More Could Be Done to Protect SSNs*, GAO-06-586T (Washington, D.C.: Mar. 30, 2006).

configuration assurance, is accomplished by verifying the correctness of the security settings on hosts, applications, and networks, and maintaining operations in a secure fashion.

FDIC did not consistently implement secure configurations of various computing devices. Specifically, the corporation did not securely configure a key production database server, desktop workstations, and handheld personal digital assistants. For example, it deployed workstations with outdated versions of third party application software. It also configured an application server and laptop computers to permit or enable the use of unnecessary applications or vulnerable services, including wireless technologies. As a result, increased risk exists that a malicious user could exploit the insecure configurations to gain unauthorized access to these devices and the information they contain.

Audit and Monitoring of Security-Related Events

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions are taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail, or logs of system activity, they can use to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which organizations configure system or security software determines the nature and extent of information that can be provided by the audit trail. To be effective, organizations should configure their software to collect and maintain audit trails that are sufficient to track security- and audit-related events.

FDIC did not sufficiently log and monitor key security- and audit- related events. For example, it did not monitor all accesses between systems for mainframe environments and FDIC did not review all changes to security administrator accounts. The corporation also did not prepare key security reports such as the failed logon attempt report and financial transaction audit logs that were critical to monitoring financial activities. Moreover, one database supporting a financial application did not have auditing enabled for changes to sensitive tables or actions taken by administrators. As a result, increased risk exists that unauthorized or inappropriate system activity may not be detected.

Physical Security

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls involve restricting physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are

housed and periodically reviewing access granted to ensure that it continues to be appropriate based on criteria established for granting such access. At FDIC, physical access control measures such as guards, badges, and alarms, used alone or in combination, are vital to safeguarding critical financial and sensitive information and computer operations from internal and external threats.

The corporation has taken steps to improve its physical security and access to its data center; nevertheless, weaknesses similar to those reported in previous audits have recurred.[20] A recently implemented consolidated physical access system did not allow the corporation to effectively track and review physical access activity to the data center. Moreover, the corporation did not adequately maintain documentation on approved access request forms. For example, 40 percent of the data center access request approvals reviewed were not current. As a result, the corporation increased the risk of inappropriate access to sensitive areas.

Weaknesses in Other Information System Controls Increase Risk

In addition to access controls, other important controls should be in place to ensure the security and reliability of an organization's information. These controls include policies, procedures, and control techniques to (1) appropriately segregate incompatible duties and (2) prevent unauthorized changes to application software. Weaknesses in these areas could increase the risk of unauthorized use, disclosure, modification, or loss of FDIC's financial and sensitive information.

Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structure that help to ensure that no single individual can independently control all key aspects of a process or computer-related operation and thereby gain unauthorized access to assets or records. Often segregation of duties is achieved by dividing responsibilities among two or more individuals or organizational groups. This division of responsibilities 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 another individual or group. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed and improper program changes could be implemented.

[20] GAO-03-629 and GAO-02-688.

FDIC did not always assure appropriate segregation of incompatible duties. It granted NFE accounts payable users inappropriate access to perform incompatible functions, such as the ability to both initiate and authorize the same transactions. Another individual performed multiple incompatible functions that included serving as an NFE security administrator, performing financial operations functions such as updating financial records and reports, and testing NFE monitoring programs. As a result, increased risk exists that erroneous or fraudulent transactions could be processed without detection.

Application Change Controls

It is important to ensure that only authorized and fully tested application programs are placed in operation. To ensure that changes to application programs are necessary, work as intended, and do not result in the loss of data or program integrity, such changes should be documented, authorized, tested, and independently reviewed. In addition, test procedures should be established to ensure that only authorized changes are made to the application's program code.

As reported in calendar year 2004, and once again recurring this year, the corporation did not consistently implement effective application change controls. FDIC has not fully developed procedures to ensure that only authorized changes were made to the production version of application code for all applications. As a result, the risk of unauthorized, untested, or inaccurate application modifications is increased and could result in unauthorized users gaining access to key financial or sensitive information.

Information Security Program Is Not Yet Fully Implemented

FDIC has made progress in developing and implementing its FISMA-mandated information security program.[21] For example, the corporation has established a memorandum of agreement and an interagency security agreement with a critical service provider, and it has implemented a program for periodically testing and evaluating the effectiveness of its information security policies, procedures, and practices.

[21]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, including those operated or maintained by contractors or others on behalf of the agency, using a risk-based approach to information security management.

However, a key reason for the weaknesses in FDIC's information system controls is that the corporation has not fully implemented elements of its information security program.

Among other things, FISMA requires agencies to develop, document, and implement the following:

- policies and procedures that cost-effectively reduce risks and ensure compliance with applicable requirements;
- plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- security awareness training to inform personnel—including contractors and other users of the agency's information systems—of information security risks and responsibilities of personnel in complying with agency policies and procedures;
- a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in their information security policies, procedures, or practices; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

A fully implemented security program is critical to providing FDIC with a solid foundation for resolving existing information security problems and continuously managing information security risks.

Policies and Procedures

A key element in implementing an effective information security program is to develop and implement risk-based policies, procedures, and controls that provide security over an agency's computing environment. Developing and documenting security policies are important because these are the primary mechanisms by which management communicates its views and requirements; they also serve as the basis for adopting specific procedures and technical controls. In addition, agencies need to take the actions necessary to effectively implement or execute these procedures and controls. If properly implemented, they can help to reduce the risk that could come from unauthorized access or disruption of services.

FDIC has documented various policies for establishing effective information security controls; however, the corporation has not

consistently implemented them. For example, policies requiring the monitoring and review of critical security events related to the mainframe computer or certain financial transactions were not always followed. The corporation also did not effectively implement policies regarding physical access, business impact analyses, sensitive Privacy Act-protected data, wireless configurations, or user account management. As a result, FDIC has less assurance that its systems and information are sufficiently protected.

Security Plans

The objective of system security planning is to improve the protection of information technology resources. A system security plan provides an overview of the system's security requirements and describes the controls that are in place—or planned—to meet those requirements. Office of Management and Budget (OMB) guidance directs agencies to develop and implement system security plans for major applications[22] and for general support systems[23] and also directs that these plans address policies and procedures for providing management, operational, and technical controls. National Institute of Standards and Technology (NIST) guidelines state that, when nonmajor applications are bundled with a general support system, the security requirements for each of the nonmajor applications should be included in the general support system's security plan. Further, agencies are responsible for ensuring that appropriate security controls are in place for the information or application, as well as the systems on which they reside. If an agency's information is processed on another organization's general support system, the agency needs to ensure that adequate protection is provided for its information, including making an assessment of the sponsoring system's security plan.

In the security plans we reviewed, FDIC generally included elements such as security controls currently in place, or planned, the name of the individual responsible for the security of the system, and a description of the system and its interconnected environment. However, we identified instances where security plans were incomplete. For example, FDIC did

[22]A major application is an application that requires special attention to security due to the risk and magnitude of the harm that could result from the loss, misuse, or unauthorized access to or modification of the information in the application.

[23]A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications.

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. As a result, FDIC cannot ensure that appropriate controls are in place to protect its systems and critical information.

Security Training

Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital that employees and contractors who use computer resources in their day-to-day operations be made aware of the importance and sensitivity of the information they manage, as well as the business and legal reasons for maintaining its confidentiality, integrity, and availability. FISMA requires that each agency provide security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks. In addition, individuals with significant responsibilities for information security should receive specialized training with respect to their responsibilities.

The corporation uses a Web-based security awareness training application and requires that all network users (employees and contractors) take the training. The application tracks users that complete the awareness training and those that do not. Users that do not take the training within required time frames are denied access to the FDIC systems. On the other hand, individuals with significant security responsibilities did not consistently receive specialized training. For example, the corporation's FISMA report for fiscal year 2005 stated that only 58 percent of such employees had received specialized training. Until FDIC ensures that each of these employees receives appropriate security training, security lapses are more likely to occur.

Remedial Actions

The development and implementation of remedial action plans are key components of an effective information security program. These plans assist agencies in identifying, assessing, prioritizing, and monitoring the progress in correcting security weaknesses that are found in information systems. FISMA says that agencies must develop a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies in the information security policies, procedures, and practices of the agency. According to OMB guidance, agencies should take timely and

effective action to correct deficiencies that they have identified through a variety of information sources. To accomplish this, remedial actions should be developed and implemented for each deficiency, and progress for each should be tracked.

FDIC has developed a process for planning and implementing remedial actions that includes the necessary elements for addressing deficiencies in information security. Indeed, we determined that FDIC has corrected 18 of the 24 deficiencies we reported as unresolved at the time of our last review. However, we found that, in some instances, FDIC did not effectively implement or accurately report the status of its remedial actions. For example, the corporation closed weaknesses identified by its security test and evaluation process without ensuring that adequate security controls were in place to resolve the weaknesses. To illustrate, it closed remedial actions for 29 logical access, 3 segregation of duties, and 6 audit log control weaknesses in the New Financial Environment (NFE) without fully testing compliance with stated security requirements. In this instance, FDIC reported the weaknesses as resolved and remedial action as complete when it established a plan to address the weaknesses, not when the corrective controls were actually implemented. In addition, tests were not performed to verify that the vulnerability was addressed by the plan's implementation. Further, the Chief Information Officer stated that, in granting NFE interim authorities to operate, the closing of high priority items related to auditing, without adequately resolving the vulnerability, resulted in a residual risk to the operations and assets of the corporation that is not fully acceptable. Without a mature remediation process, the corporation cannot ensure that the organization's weaknesses are mitigated to reduce risks.

Continuity of Operations

Continuity of operations controls should be designed to ensure that, when unexpected events occur, essential operations continue without interruption or can be promptly resumed, and critical and sensitive data are protected. These controls include environmental controls and procedures designed to protect information resources and minimize the risk of unplanned interruptions, along with a well-tested plan to recover critical operations should interruptions occur. NIST recommends that a formal business impact analysis be performed to allow management to better understand and measure the financial and nonfinancial risks associated with the potential loss of any mission-critical system. Corporation policy requires that a business impact analysis be conducted as frequently as changing conditions mandate, but that a review of the analysis should be conducted no less than annually. This analysis is an essential step in the

process to develop and test contingency plans since the impact analysis establishes the risks associated with disruption and helps prioritize the recovery process. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and financial or management information to be inaccurate or incomplete.

FDIC did not update its business impact analysis to reflect the significant changes resulting from the implementation of the New Financial Environment; consequently, the continuity plans and testing do not reflect the current environment. We previously reported a similar business impact analysis weakness in the corporation's information security controls.[24] Although FDIC performed a limited disaster recovery test for the New Financial Environment, the April 2005 test was conducted prior to implementation of the new production system. Further, at the time of our review, the corporation had not tested the new production environment. Without a current business impact analysis for the new system and the successful restoration of the new production environment, the corporation cannot ensure that NFE will be recovered in a timely manner in the event of a disaster.

Conclusions

While FDIC has made progress in addressing our previous recommendations, information security weaknesses continue to impair the corporation's ability to ensure the confidentiality, integrity, and availability of financial and other sensitive data. The severity of these weaknesses was such that we reported information system control weaknesses to be a reportable condition in our 2005 financial audit report[25] since financial and sensitive information are at increased risk of unauthorized access, modification, and/or disclosure, possibly without detection. Until FDIC fully implements key security control elements that include enhanced access permissions, system monitoring, physical access, and continuity of operations, its facilities and computing resources and the information that is processed, stored, and transmitted on its systems will remain vulnerable to unauthorized access, modification, or destruction.

[24]GAO-03-629.

[25]GAO-06-146.

Recommendations for Executive Action

To help fully implement the corporation's information security program, we recommend that the FDIC Chairman take the following five actions:

- consistently implement the corporation's documented policies and procedures related to information security,
- include security plans or requirements for nonmajor applications into the plans for general support systems,
- provide specialized training to individuals with significant security responsibilities,
- report weaknesses as closed in remedial action plans only when corrective actions have been completed, and
- update continuity of operations plans and test them for the New Financial Environment.

We are also making recommendations in a separate report designated for "Limited Official Use Only."[26] These recommendations address actions needed to correct specific information security weaknesses related to access and other information system controls.

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 (these are reprinted in app. I). In these comments, the Deputy acknowledged the benefit of the recommendations made as a part of this year's audit and provided examples of actions that FDIC has taken with regard to security. The Deputy stated that FDIC concurred with one of our recommendations, partially concurred with three, and did not concur with one. He also stated that FDIC disagreed with our assessment that its information system control weaknesses were sufficient to constitute a reportable condition.

According to the Deputy, FDIC agreed with our recommendation that it include security plans or requirements for nonmajor applications into the plans for general support system and stated that it had added these applications into such security plans. However, the Deputy questioned the

[26]GAO-06-619SU.

need for the corporation to assess the security plans for its payroll service provider (the National Finance Center), as we had stated in a draft of this report. FDIC considers that such effort on its part would be duplicative, because its payroll service provider is federally certified and audited by the Department of Agriculture's Inspector General, and FDIC reviews the IG assessments. In addition, the Deputy stated that the corporation has secured the appropriate agreements required for interconnections of systems, as required by NIST. We agree with the FDIC position and have revised the report accordingly.

With regard to our recommendation that FDIC consistently implement the corporation's documented policies and procedures related to information security, FDIC partially concurred. The corporation agreed with some aspects of our analysis and took remedial action, such as removing certain inactive accounts from computers, in conformance with corporation policy. However, FDIC did not agree with other aspects of our assessment. For example, we identified a machine in FDIC's security testing lab as not compliant. According to the Deputy, the risk from this vulnerability was fully mitigated because the machine was not a production computer, and software was implemented to prevent simultaneous connection to the production network and to wireless computing network. We disagree that these conditions fully mitigate the risk posed by this vulnerability: in certain circumstances, one vulnerable machine on a network could be used to gain access to related networks and compromise the confidentiality, integrity, and availability of information and information systems as a whole. Even with mitigating controls, such vulnerability increases risk.

With regard to our recommendation that FDIC provide specialized training to individuals with significant security responsibilities, FDIC partially concurred. The corporation acknowledged that a "small subset" of employees with significant security responsibilities did not attend the originally scheduled specialized training; however, according to the Deputy, these employees have since attended training or were provided with training materials. Accordingly, FDIC believes that it is now in compliance with this recommendation. As stated in our report, FDIC reported that only 58 percent of such employees had received specialized training. If the remaining 42 percent have now received the appropriate training, FDIC will have satisfied our recommendation.

With regard to our recommendation that FDIC update its continuity of operations plans and test them for the New Financial Environment, FDIC partially concurred. According to the Deputy, the corporation has now

updated its Business Impact Analysis (on which its continuity of operations plans are based), and it retested its disaster recovery program in 2006, including a full test of the New Financial Environment. Accordingly, FDIC believes that it is now in compliance with this recommendation. The Deputy described the corporation's concurrence as partial because of the timing of several events, including the corporation's response to Hurricane Katrina and other priorities. According to the Deputy, FDIC had exercised its discretion in continuing to rely on its previous Business Impact Analysis because of these other priorities. In addition, the Deputy stated that although the corporation did not test the New Financial Environment in a production environment, it ran a limited test of the system before it went into production. At the time of our review, however, the Business Impact Analysis did not reflect the current environment, which had been significantly changed as a result of the implementation of the New Financial Environment. An outdated Business Impact Analysis increases risk because this analysis provides a mechanism for identifying the business functions that will be affected by availability problems and thus forms the basis for disaster recovery planning and testing. FDIC's recent actions to address this risk are thus important; although we have not evaluated these actions, if they have been implemented appropriately, FDIC will have satisfied our recommendation.

FDIC did not concur with our recommendation that it report weaknesses as closed in remedial action plans only when corrective actions are taken. According to the Deputy, the corporation disagreed with the assessment on which this recommendation was based: that is, that it did not effectively implement or accurately report the status of remedial actions. According to FDIC, our observation was based on a single instance that was part of a pilot test process, and thus the finding was not valid for the program that was in place through most of 2005. However, we disagree with FDIC's characterization that our observation was based on a single instance. Our finding is based on a remediation plan that FDIC developed following a security test and evaluation of its New Financial Environment. In that plan, dated November 2005, we found 38 control weaknesses that were closed without test or validation. FDIC also provided us with an updated remediation plan for this test, dated December 2005, which did not include the improperly closed weaknesses or any indication that they had been addressed. We also disagree that our finding was not valid for the process that was in place for most of 2005. Our analysis was based on the process in

effect from March to December 2005.[27] Further, several of the items that were improperly closed were the same weaknesses that we identify in this report. For example, we found that the corporation closed weaknesses that had been identified in areas such as security awareness training, segregation of duties, encryption, and audit and monitoring; however, during our audit we found that these weaknesses still existed.

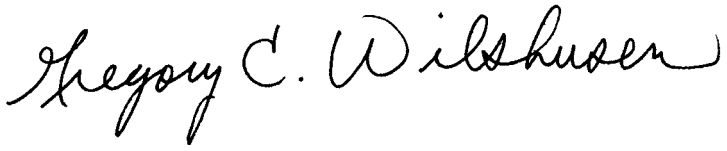
After the end of the review period, FDIC informed us that it was improving its process to ensure that weaknesses were not closed without corrective action, but we have not evaluated this improved process. In his comments, the Deputy stated that FDIC is now in compliance with our recommendation, because its mature program requires full monitoring of remedial actions and testing for completion. If FDIC's process has been implemented appropriately, the corporation will have satisfied our recommendation.

Finally, the FDIC does not share our assessment that it had a reportable condition due to the severity of the risk impact or the magnitude of the collective vulnerability posed by potential control issues. However, we believe that the problems we identified in this report concerning FDIC's security program adversely affected the overall security posture of the corporation and did merit a reportable condition. These problems included the (1) lack of consistent implementation of documented policies and procedures related to information security, (2) absence of integration of nonmajor applications into general support security plans, (3) lack of specialized security training for trusted employees, (4) an oversight process that allowed weaknesses to remain open even though they were reported as closed, (4) lack of updated Business Impact Analyses and contingency plans, (5) failure to test the New Financial Environment in a production environment, and (6) significant access controls vulnerabilities described in a separate report. All of these vulnerabilities contributed to our reinstating a reportable condition on FDIC information security controls.

[27]The New Financial Environment remediation process that we reviewed was in place from March to December 2005. The first release of the New Financial Environment underwent a security test and evaluation that was completed in March 2005; we reviewed a copy of the resulting remediation plans, dated November 2005, as well as an updated copy, dated December 2005. In addition, the second release of the New Financial Environment underwent a security test and evaluation that was completed in June 2005. We also reviewed the remediation plan, dated November 2005, that resulted from this test.

We are sending copies of this report to the Chairman and Ranking Minority Member of the Senate Committee on Banking, Housing, and Urban Affairs; the Chairman and Ranking Minority Member of the House Committee on Financial Services; members of the FDIC Audit Committee; officials in FDIC's divisions of information resources management, administration, and finance; and the FDIC inspector general. 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 me at (202) 512-6244 or by e-mail at wilshuseng@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 II.



Gregory C. Wilshusen
Director, Information Security Issues

Comments from the Federal Deposit Insurance Corporation

FDIC
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Deputy to the Chairman and CFO

August 18, 2006

Mr. Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office
Washington, D.C. 20548

Re: FDIC Management Response to the GAO 2005 Audit of FDIC's Information Security Program

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the U.S. Government Accountability Office's (GAO) draft audit report titled, Information Security: Federal Deposit Insurance Corporation Needs to Improve Its Program, GAO-06-620. 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 2004, 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 2005. As a leading agency in information security, our goal at the FDIC is to work diligently and constructively with the GAO during the upcoming 2006 audit to remove the reportable condition that was reinstated during the 2005 reporting process.

We are pleased to accept GAO's acknowledgement of the progress FDIC has made in correcting previously reported weaknesses. These improvements include developing and implementing procedures to comply with its computer file name convention standards, and developing and implementing automated procedures for limiting access to sensitive information. 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. In addition to those improvements identified in the report, we would like to point out a number of other significant improvements accomplished over the last three years that we believe provide additional insight into the strength and maturity of our information security program. The FDIC has:

- Strengthened security policies and procedures covering all GAO Federal Information System Controls Audit Manual (FISCAM) areas
- Enhanced management oversight through the implementation of a CIO Council
- Re-organized, fully staffed and modernized the Information Security Staff
- Implemented a National Institute of Standards and Technology (NIST) compliant Risk Assessment and Management Program
- Implemented a NIST compliant Certification and Accreditation Program
- Implemented a NIST compliant Security Test and Evaluation Program

- Implemented an independent Self Assessment Program including quarterly sweeps of FDIC networks and servers
- Implemented a 24x7 Monitoring Program including:
  - Intrusion Detection (Computer Security Incident Response Team (CSIRT) and scan programs)
  - Security Patch Management
  - Firewall Protection
- Implemented significant enhancements to the Corporate Privacy Awareness Program
- Completed a Technical Infrastructure Modernization Program that provides more robust security controls
- Formed Collaborative Working Groups which provide for the identification of sensitive data
- Enhanced the Corporate Security Awareness Training Program
- Enhanced the Business Continuity and Disaster Recovery Programs including a new and expanded backup and recovery site.
- Enhanced remote access security with 2 factor authentication
- Integrated security controls into the Rational Unified Process (RUP) Application Life Cycle Development Program
- Incorporated Security Architecture planning within the Enterprise Architecture Program
- Integrated security into the Application and Infrastructure Testing Programs including:
  - Independent testing
  - NSA penetration testing
- Improved project and cost management controls including:
  - Capital Investment Reviews
  - Program Management Office

Over the past several years, the FDIC and the GAO have enjoyed a cordial and mutually beneficial relationship. Through our joint efforts, we have made numerous improvements to strengthen our information security program. As a result of these improvements, the FDIC is also pleased that the GAO has directly or indirectly referred the Securities and Exchange Commission (SEC), U.S. Forest Service, Office of the Comptroller of the Currency (OCC), Federal Reserve Board (FRB), National Labor Relations Board (NLRB), and National Science Foundation (NSF) to us for advice on aspects of their security programs. Indeed, GAO sought out the FDIC's expertise on combating phishing and internal scams within the last year. It is with great pride that we acknowledge GAO's recognition of the many positive components of our comprehensive information security program. As an agency, we are committed to maintaining this leadership position in the field of information security.

In addition to the recommendations detailed in the limited distribution version of this report, GAO's report recommends the FDIC execute five actions to address GAO's concerns. Our public response addresses these five actions. Additional materials are provided in our response to the limited distribution report including a clarification pertaining to a prior year issue

previously communicated to GAO and included in the details of that response. At this time, the FDIC concurs with one, partially concurs with three others, and is unable to concur with the remaining action. Specifically, the GAO recommended that the FDIC:

- Consistently implement the corporation's documented policies and procedures related to information security.

  FDIC response: The recommendation is based upon multiple findings detailed in the limited distribution version of this report, several of which we do not agree with. As such, the FDIC partially concurs with this recommendation. For example, we agree that we did not always remove certain inactive accounts from our computers in a timely manner, as is our policy. These accounts have now been removed and we will continue to monitor compliance. However, we do not agree with GAO's assessment of the FDIC's compliance with our policy on wireless technology configuration. The GAO identified a single machine that was shown to be located in our security testing lab for known security testing. This machine was not a production computer nor was it on the FDIC production network. Thus it represented no threat to the agency. The FDIC has implemented a new software product in our production environment which prevents simultaneous connection to the FDIC production network and to a wireless computing network, fully mitigating the issue cited by the GAO team. FDIC also partially agrees with the need to improve monitoring of the mainframe and the New Financial Environment (NFE); however, we believe the risk and impact of this finding is significantly overstated given the layers of other mitigating controls already in place. Still, the FDIC recognizes that audit reports can be improved to make it easier to review access by logging and monitoring. FDIC is in the process of implementing the required monitoring procedures and report mechanisms. Our detailed responses to the other policy areas mentioned are provided under separate cover in our response to the limited distribution version of this report.

- Include security plans or requirements for non-major applications into the plans for general support systems.

  FDIC response: This recommendation stems from the audit team's assessment that the FDIC had some security plans that were incomplete. FDIC concurs with this revised recommendation, and, in fact, has independently implemented, subsequent to the GAO audit, the inclusion of non-major applications into security plans for general support systems. However, we do not concur with the related text on page 19 of the GAO draft audit report which states "the corporation did not obtain or assess the security plan for its payroll service provider". The FDIC has secured the appropriate agreements required for interconnection of systems per NIST. In addition, the National Finance Center (NFC), as part of the Department of Agriculture, is a federally run and federally audited environment. We see no benefit in the FDIC duplicating the efforts of another federal agency. The Certification Agent for NFC certifies the NFC payroll system to operate and has given a full certification to operate. In addition, the FDIC has reviewed a U.S. Department of Agriculture

Inspector General's assessment of the NFC and has put in place the necessary interconnection agreements with this agency.

- Provide specialized training to individuals with significant security responsibilities.

  FDIC response: This recommendation stems from the audit team's assessment that the FDIC had individuals with significant security responsibilities that did not receive specialized training in 2005. We partially concur with that assessment. The specialized training was fully operational during 2005. We acknowledge that a small subset of employees and contractors were not able to attend at the originally scheduled time, but would point out that they were included in follow-up training or were provided with training materials and required to sign a statement that they had read and understood their security responsibilities. In addition, all FDIC employees and contractors must complete annual privacy and security awareness training. If they fail to complete any of this training their access to FDIC systems is revoked. As such, the FDIC believes we are now in compliance with this recommendation.

- Report weaknesses as closed in remedial action plans only when corrective actions have been completed.

  FDIC response: This recommendation stems from the audit team's assessment that the FDIC did not effectively implement or accurately report the status of remedial actions. We do not concur with that assessment. The finding is based upon a single instance and is not valid for the program that was in place for most of 2005. FDIC provided GAO with additional documentation showing that follow-up activities had addressed the initial weaknesses. The finding is based upon observations of a "pilot" test process for NFE. NFE was subsequently included in a follow-up security test and evaluation and successfully passed for all areas tested. The mature program requires full monitoring and compliance testing for completion of all findings identified. As such, the FDIC believes we are already in compliance with this recommendation.

- Update continuity of operations plans and test them for NFE

  FDIC response: This recommendation stems from the audit team's assessment that the FDIC continuity of operations plans were not up to date, including business impact analysis and NFE was not tested under these plans. We partially concur with that assessment based upon the timing of the following events. During 2005, due to the federal agency response required by the Hurricane Katrina disaster and by several other priority initiatives, FDIC management exercised its discretion to continue to rely upon the Business Impact Analysis performed in 2004. The FDIC performed an annual Disaster Recovery test in April 2005, which included a limited test of the NFE even though the NFE application had not yet been installed into production use. As a result of the corporation's fall 2005 decision to relocate its recovery backup site, FDIC management exercised its discretion to not incur the expenses and divert the resources to retest our Disaster Recovery capability prior to this move. The FDIC has

a well established program for the maintenance and testing of our continuity of operations plans including Business Impact Analyses and has done so for a number of years. The Business Impact Analysis has been updated and the disaster recovery plans have been successfully retested in 2006 under this program. This test included a full test of NFE. As such, the FDIC believes we are now in compliance with this recommendation.

With regard to the reinstated reportable condition on information systems controls, we respectfully acknowledge but do not share the GAO's assessment of the severity of the risk impact or the magnitude of the collective vulnerability posed by the potential control issues identified by the GAO's audit team. Nevertheless, at this point, we believe we have addressed many of the concerns GAO highlighted in its reports and are aggressively pursuing completion of the remaining actions by year-end. Further, the FDIC's confidence in the sufficiency of our information systems environment and the related information systems controls is grounded in what we believe is a deliberate, comprehensive security program designed, in conjunction with the deployment of NFE, to integrate not only system controls, but procedural, managerial, and audit controls into a balanced and cost-effective control framework. Notwithstanding any remaining differences in our assessments of the FDIC's IT security environment, the FDIC looks forward to working diligently with our GAO audit partners, throughout the 2006 audit cycle, to reconcile our respective views on these matters and to augment our IT security program and practices in those instances where it is determined that changes are appropriate.

Once again, we thank you for your past contributions and your work on this year's audit. We look forward to continued discussions with the GAO on each of the issues raised in the 2005 audit, and to working with the GAO towards a common understanding and approach to continuing to improve our information security program.

If you have any questions or concerns, please do not hesitate to contact me.

Sincerely,

Steven O. App

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

5

GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen (202) 512-6244

Staff Acknowledgments

In addition to the individual named above, the following people made key contributions to this report: William Wadsworth; Ed Alexander, Jr.; Gerald Barnes; Angela Bell; Mark Canter; Jason Carroll; Lon Chin; Barbara Collier; Anh Dang; Kristi Dorsey; Denise Fitzpatrick; Ed Glagola; Nancy Glover; David Hayes; Sairah Ijaz; Kevin Metcalfe; Duc Ngo; Tammi Nguyen; Eugene Stevens; Charles Vrabel; and Chris Warweg.

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 "Subscribe to 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, D.C. 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

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548