

GAO

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

May 2007

INFORMATION SECURITY

Federal Deposit Insurance Corporation Needs to Sustain Progress Improving Its Program





Highlights of [GAO-07-351](#), 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. As part of its audit of the calendar year 2006 financial statements, GAO assessed (1) the progress FDIC has made in correcting or mitigating information security weaknesses previously reported and (2) the effectiveness of FDIC's system integrity controls to protect the confidentiality and availability of its financial information and information systems.

To do this, GAO examined pertinent security policies, procedures, and relevant reports. In addition, GAO conducted tests and observations of controls in operation.

What GAO Recommends

GAO recommends that FDIC take actions to address control weaknesses and fully integrate the NFE into the corporation's information security program. In written comments on a draft of this report, FDIC's Deputy to the Chairman and Chief Financial Officer stated that FDIC concurred with seven of GAO's recommendations and partially concurred with five and has implemented or will implement corrective actions. If the corporation adequately implements these actions, it will have satisfied the intent of GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-351.

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

INFORMATION SECURITY

Federal Deposit Insurance Corporation Needs to Sustain Progress Improving Its Program

What GAO Found

FDIC has made substantial progress in correcting previously reported weaknesses in its information security controls. Specifically, it has corrected or mitigated 21 of the 26 weaknesses that GAO had reported as unresolved at the completion of the calendar year 2005 audit. Actions FDIC has taken include developing and implementing procedures to prohibit the transmission of mainframe user and administrator passwords in readable text across the network, implementing procedures to change vender-supplied account/passwords, and improving mainframe security monitoring controls.

Although FDIC has made important progress improving its information system controls, old and new weaknesses could limit the corporation's ability to effectively protect the integrity, confidentiality, and availability of its financial and sensitive information and systems. In addition to the five previously reported weaknesses that are in the process of being mitigated, GAO identified new weaknesses in controls related to (1) e-mail security, (2) physical security, and (3) configuration management. 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 and sensitive systems and information.

In addition, FDIC has not fully integrated its new financial system—the New Financial Environment (NFE)—into its information security program. For example, it did not fully implement key control activities for the NFE. Until FDIC fully integrates the NFE with the information security program, its ability to maintain adequate system controls over its financial and sensitive information will be limited.

Contents

| | | |
|---------------------|--|-----------|
| Letter | | 1 |
| | Results in Brief | 2 |
| | Background | 3 |
| | Objectives, Scope, and Methodology | 6 |
| | FDIC Has Made Substantial Progress Correcting Previously Reported Weaknesses | 8 |
| | FDIC Has Made Progress in Information System Controls, However Some Weaknesses Remain | 9 |
| | NFE Not Fully Integrated into the Corporation's Information Security Program | 11 |
| | Conclusions | 14 |
| | Recommendations for Executive Action | 15 |
| | Agency Comments and Our Evaluation | 16 |
| Appendix I | Status of Previously Reported Weaknesses | 18 |
| Appendix II | Comments from the Federal Deposit Insurance Corporation | 20 |
| Appendix III | GAO Contact and Staff Acknowledgments | 32 |

Abbreviations

| | |
|-------|--|
| CSIRT | Computer Security Incident Response Team |
| BIF | Bank Insurance Fund |
| DIF | Deposit Insurance Fund |
| 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 |
| SAIF | Savings Association Insurance Fund |
| SAS | Statement on Auditing Standards |

This is a work of the U.S. government and is not subject to copyright protection in the United States. It 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 18, 2007

To the Chief Financial Officer 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 integrity, confidentiality, 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 2006 financial statements of the Deposit Insurance Fund² (DIF) and the Federal Savings & Loan Insurance Corporation (FSLIC) Resolution Fund,³ we assessed (1) the progress FDIC has made in correcting or mitigating information system control weaknesses reported as unresolved at the completion of our 2005 review⁴ and (2) the effectiveness of the corporation's information system controls

¹Information system internal controls affect the overall effectiveness and security of computer operations and are not unique to specific computer applications. 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.

²Bank Insurance Fund (BIF) and the Savings Association Insurance Fund (SAIF) merged to become the DIF.

³GAO, *Financial Audit: Federal Deposit Insurance Corporation Funds' 2006 and 2005 Financial Statements*, [GAO-07-371](#) (Washington, D.C.: Feb. 13, 2007).

⁴GAO, *Information Security: Federal Deposit Insurance Corporation Needs to Improve Its Program*, [GAO-06-620](#) (Washington, D.C.: Aug. 31, 2006) and 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).

for protecting the confidentiality, integrity, and availability of its information and information systems.

In our audit report⁵ on the calendar year 2006 financial statements of the FDIC's funds, we concluded that issues related to information security controls do not constitute a significant deficiency.⁶ We also stated in that report that continued management commitment to an effective information security program will be essential to ensure that the corporation's financial and sensitive information will be adequately protected.

We performed our review at the FDIC computer facility in Arlington, Virginia, from September 2006 through February 2007. Our review was performed in accordance with generally accepted government auditing standards.

Results in Brief

FDIC has made substantial progress in correcting previously reported weaknesses. Specifically, it has corrected or mitigated 21 of the 26 weaknesses that we had reported as unresolved at the completion of our calendar year 2005 audit. Actions that FDIC has taken include developing and implementing procedures to prohibit the transmission of mainframe user and administrator passwords in plaintext across the network, implementing procedures to change vendor-supplied account/passwords, and improving mainframe security monitoring controls.

Although it has made important progress improving its information system controls, weaknesses exist that could limit FDIC's ability to effectively protect the confidentiality, integrity, and availability of its financial and sensitive information and systems. In addition to the five previously reported weaknesses that are in process of being addressed, we identified new information security weaknesses. For example, the corporation did not consistently implement controls related to (1) e-mail security, (2)

⁵[GAO-07-371](#).

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. As a result of Statement on Auditing Standards (SAS) 112, the term reportable condition is no longer used.

physical security, and (3) configuration management. Although these weaknesses do not pose a significant risk of misstatement of the corporation's financial statements, they do increase preventable risk to the corporation's financial and sensitive systems and information.

In addition, FDIC has not fully integrated its new financial system—called the New Financial Environment (NFE)—into its information security program. Although FDIC had developed, documented, and implemented a corporate information security program, it did not fully implement key control activities for the NFE. For example, FDIC had not sufficiently assessed risks, updated the security plan, reported certain security incidents, or updated the contingency plan. Until FDIC fully integrates the NFE with the information security program, its ability to maintain adequate system controls over its financial and sensitive information will be limited.

We are recommending that the FDIC Chief Financial Officer and Chief Operating Officer take actions to address the control weaknesses and to fully integrate the NFE into the corporation's information security program.

In written comments on a draft of this report (which are reprinted in app. II), FDIC's Deputy to the Chairman and Chief Financial Officer stated that FDIC concurred with seven of our recommendations and has implemented or will implement them in the coming year. FDIC partially concurred with our remaining five recommendations and, based on the Deputy's comments, we have made revisions to and clarified one of the recommendations. The Deputy stated that the corporation has developed or implemented plans to adequately address the underlying risks that prompted these five recommendations, in some instances through alternative corrective actions. If the corporation effectively implements these corrective actions, it will have satisfied 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. 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 have changed the way our government, the nation, and much of the world communicate and conduct business. However, 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. This concern is 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. Thus, we have designated information security as a governmentwide high-risk area since 1997,⁷ a designation that remains today.⁸

Recognizing the importance of securing federal agencies' information and systems, Congress enacted the Federal Information Security Management Act of 2002 (FISMA) to strengthen the security of information and systems within federal agencies.⁹ FISMA requires each agency to use a risk-based approach to develop, document, and implement a departmentwide information security program for the information and systems that support the operations and assets of the agency.

FDIC Is a Key Protector of Bank and Thrift Depositors

Congress created FDIC in 1933¹⁰ 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.¹¹ The act designated FDIC as the administrator of two funds responsible for protecting insured bank and thrift depositors—BIF and the SAIF. The act also designated FDIC as the administrator of the FSLIC Resolution Fund, which was created to complete the affairs of the former FSLIC and liquidate the

⁷GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997).

⁸GAO, *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 (Dec. 17, 2002).

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

¹¹Pub. L. No. 101-73, (Aug. 9, 1989).

assets and liabilities transferred from the former Resolution Trust Corporation. On February 8, 2006, the President signed into law the Federal Deposit Insurance Reform Act of 2005. Among its provisions, the act calls for the merger of the BIF and SAIF into the DIF.¹² FDIC completed this merger on March 31, 2006. In managing these funds, the corporation has an examination and supervision program to monitor the safety of deposits held in member institutions.

FDIC insures deposits in excess of \$4 trillion for its 8,693 member institutions. FDIC had a budget of about \$1.06 billion for calendar year 2006 to support its activities in managing the funds. For that year, it processed almost 21 million financial transactions.

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 the NFE and several financial systems that process and track financial transactions, including premiums paid by its member institutions and disbursements made to support operations. Other systems maintain personnel information for employees, examination data for financial institutions, and legal information on closed institutions. At the time of our review, there were about 5,629 users on FDIC systems.

Federal law delineates responsibilities for the management of computer systems at FDIC. Under FISMA, the Chairman of FDIC is responsible for, among other things, (1) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the 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.

Two deputies to the Chairman—the Chief Financial Officer and Chief Operating Officer—also have information security responsibilities. The

¹²Pub. L. No. 109-171, §2102 (Feb. 8, 2006).

Chief Financial Officer is responsible for the preparation of financial statements and ensures that they are fairly presented and demonstrate discipline and accountability. The Chief Financial Officer is part of a senior management group that oversees the NFE. The group receives monthly system progress updates from the NFE project team.

The Chief Operating Officer is responsible for planning, coordinating, evaluating, and improving programs and resource management. He is also in charge of the Chief Information Officer, who 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 2005¹³ and (2) the effectiveness of the corporation's information system controls for protecting the confidentiality, integrity, and availability of financial and sensitive data. An integral part of our objectives was to support the opinion on internal control in GAO's 2006 financial statement audit by assessing the degree of security over systems that support the generation of the FDIC funds' financial statements.

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;

¹³GAO-06-620 and GAO-06-619SU.

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

-
- 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;
 - 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; and
 - ensure the implementation of secure and effective configuration management.

In addition, we evaluated aspects of FDIC's information security program as they relate to NFE. 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 fieldwork. In addition, we conducted tests and observations of controls in operation 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 the FDIC computer facility in Arlington, Virginia, from September 2006 through February 2007. Our review was

¹⁵[GAO-06-620](#) and [GAO-06-619SU](#).

performed in accordance with generally accepted government auditing standards.

FDIC Has Made Substantial Progress Correcting Previously Reported Weaknesses

FDIC has taken steps to address security control weaknesses. The corporation has corrected or mitigated 21 of the 26 weaknesses that we previously reported as unresolved at the completion of our calendar year 2005 audit (see app. I). For example, the corporation has

- developed and implemented procedures to prohibit the transmission of mainframe user and administrator passwords in plaintext across the network,
- established and implemented a process to monitor and report on vendor-supplied account/password combinations, and
- improved mainframe security monitoring controls.

While the corporation has made important progress in strengthening its information security controls, it is still in the process of completing actions to correct or mitigate the remaining five previously reported weaknesses. These uncorrected actions include ensuring that only authorized application software changes are implemented, limiting network access to sensitive personally identifiable and business proprietary information, effectively generating and reviewing the NFE audit reports, adequately controlling physical access to the Virginia Square building, and properly segregating incompatible system-related functions, duties, and capacities for an individual associated with the NFE. Not addressing these actions could leave the corporation's sensitive data vulnerable to unauthorized access and manipulation.

Appendix I 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.

FDIC Has Made Progress in Information System Controls, However Some Weaknesses Remain

Although FDIC made substantial improvements to its information system controls, unresolved and newly identified weaknesses could limit its ability to effectively protect the confidentiality, integrity, and availability of its financial and sensitive information and information systems. Specifically, we identified new weaknesses in controls related to (1) e-mail security, (2) physical security, and (3) configuration management. Although these control weaknesses do not pose significant risks of misstatement to the financial reports, they do increase the risk to FDIC's financial and sensitive systems and information and increase the risk of unauthorized modification of data and programs, inappropriate disclosure of sensitive information, or disruption of critical operations.

E-mail Security

E-mail is perhaps the most popular system for exchanging business information over the Internet or any other computer network. Because the computing and networking technologies that underlie e-mail are widespread and well-known, attackers are able to develop attack methods to exploit security weaknesses. E-mail messages can be secured in various ways including the use of digital signatures. Digital signatures can be used to ensure the integrity of an e-mail message and confirm the identity of its sender. National Institute of Standards and Technology (NIST) guidance recommends that organizations consider the implementation of secure e-mail technologies such as digital signatures to ensure the integrity of e-mail data. FDIC policy requires individual division managers to establish specific procedures regarding the use of secure e-mail technologies for e-mail.

FDIC did not use secure e-mail methods to protect the integrity of certain accounting data transferred over an internal communication network. The corporation relied upon unsecured e-mail transmission of accounting data instead of using more secure methods, such as securing e-mail with digital signatures or using the internal data transmission functions in NFE. Specifically, it did not use secure e-mail correspondence during monthly NFE closing processes because the Division of Finance—the division responsible for the financial environment—had not developed requirements for securing e-mail. In addition, the e-mail system could be compromised by sending e-mails using forged sender names and addresses. As a result, increased risk exists that an attacker could manipulate accounting data.

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. FDIC policy also requires that visitors be allowed to enter an office only after providing proof of identity, identifying the person they are visiting, signing a visitor log, obtaining a visitor badge, and being escorted at all times by the employee whom they are visiting.

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. In addition, a workstation that had access to a payroll system was located in an unsecured office. As a result, increased risk exists that unauthorized individuals could gain physical access to a key facility and to systems that have sensitive information.

Configuration Management

Configuration management involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. The agency should have configuration management controls to ensure that only authorized changes are made to such critical components. In addition, all applications and changes to those applications should go through a formal, documented systems development process that identifies all changes to the baseline configuration. Also, procedures should ensure that no unauthorized software is installed. Patch management, a component of configuration management, is an important element in mitigating the risk associated with software vulnerabilities. Up-to-date patch installations help mitigate vulnerabilities associated with flaws in software code that could be exploited to cause significant damage. FDIC policy requires that patches be implemented within the specified time frames. In addition, FDIC policy states that configuration status accounting and configuration auditing, which includes both functional and physical audits, should be performed. Configuration audits help to maintain the integrity of the configuration baseline as well as to ensure that when a significant product change is introduced, only authorized changes are being made. FDIC policy also states that project documentation should be managed and updated as it evolves over time.

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;
 - ensure that all significant system changes, such as parameter changes, go through a change control process;
 - apply comprehensive patches to system software in a timely manner. For example, a FDIC report stated that in the third quarter of fiscal year 2006, software patches for 15 out of 21 high-risk vulnerabilities and 5 out of 34 medium-risk vulnerabilities were not implemented within required time frames. In another report, between July 9, 2006, and October 9, 2006, out of nine high-risk patches that were not implemented within the required time period, eight were not implemented for 42 days.
 - review status accounting reports, or perform complete functional and physical configuration audits; and
 - update or control documents to reflect the current state of the environment and to ensure consistency with related documents. Specifically, documents such as the NFE security plan, risk assessment, and contingency plan did not reflect the current environment.

The NFE project team did not institute the above because it did not always consistently follow the processes as outlined in the NFE configuration management plan. According to FDIC officials, they were not following the plan because it has not been updated to reflect the new system development life cycle. In addition, according to an FDIC official, patches were not implemented in the specified time frames because contractors do not always follow FDIC policy.

As a result, the corporation has a higher risk that NFE may not perform as intended.

NFE Was Not Fully Integrated into the Corporation's Information Security Program

Although FDIC had taken steps to develop, document, and implement a corporate information security program, it did not fully implement key control activities for NFE. For example, FDIC had not sufficiently assessed risks, updated the security plan, reported computer security incidents, or updated the contingency plan to reflect the current environment for NFE.

Risk Assessments

Identifying and assessing information security risks are essential steps in determining what controls are required. Moreover, by increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted in order to help ensure that they operate as intended. Security testing and evaluation can be used to efficiently identify system vulnerabilities for use in a risk assessment. NIST guidance states that the risk assessment should be updated to reflect the results of the security test and evaluation.

The risk assessment for NFE was not properly updated. FDIC performed a security test and evaluation after the risk assessment was performed. However, the risk assessment was not updated to include the risks associated with any of the newly identified vulnerabilities. As a result, NFE may have inadequate or inappropriate security controls that might not address the system's true risk.

Security Plans

A 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. Common security controls are controls that can be applied to one or more organizational information systems. System-specific controls are the responsibility of the information system owner. NIST guidance states that system security plans should clearly identify which security controls have been designated as common security controls and the individual responsible for implementing the common security control. In addition, NIST guidance states that organizations should update information system security plans to address system/organizational changes.

The corporation did not update the system security plan for NFE. FDIC has identified 77 management, operational, and technical common security controls established in its information system. However, the NFE security plan was not updated to clearly identify common security controls. In addition, the security plan was not updated to reflect the correct servers or recently installed mainframe hardware. As a result, increased risk exists that proper controls may not be implemented for the NFE.

Incident Handling

Even strong controls may not block all intrusions and misuse, but organizations can reduce the risks associated with such incidents if they take steps to promptly detect and respond to them before significant damage is done. In addition, analyzing security incidents allows

organizations to gain a better understanding of the threats to their information and the costs of their security-related problems. Such analyses can pinpoint vulnerabilities that need to be eliminated so that they will not be exploited again. FISMA requires that agency information security programs include procedures for detecting and reporting security incidents. NIST guidance states that organizations should implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. In addition, NIST guidance states that organizations should regularly review and analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions. FDIC policy requires all users of the corporate information systems to report suspected computer security incidents¹⁶ to the Computer Security Incident Response Team (CSIRT).

FDIC has implemented an incident handling program, including establishing a team and associated procedures for detecting, responding to, and reporting computer security incidents. However, the corporation did not always review events occurring in the NFE to determine whether the events were computer security incidents or not. For example, during our observation of the purchase order matching process, an FDIC official overrode a matching exception. Although an override exception matching report was generated, it was not reviewed to determine if it was an incident, and was not forwarded to CSIRT. According to an official, there were not always procedures to review events in NFE. As a result, increased risk exists that computer security incidents that relate to the NFE will not be identified.

Continuity of Operations

Continuity of operations, which includes disaster recovery planning, 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 procedures to minimize the risk of unplanned interruptions, along with a well-tested plan to recover critical operations should interruptions occur. FISMA requires that agencies have plans and procedures to ensure

¹⁶FDIC policy defines a computer security incident as an event that threatens the security of the corporate information systems, including FDIC's computers, mainframe, networks, software and associated equipment, and information stored or transmitted using that equipment.

the continuity of operations for information systems that support the operations and assets of the agency. NIST guidance states that disaster recovery plans, including contingency plans, should be maintained in a ready state that accurately reflects system requirements, procedures, and organizational structure.

FDIC has developed plans for the continuity of NFE operations. To assess the effectiveness of the plans, FDIC successfully tested the NFE at its new disaster recovery site.¹⁷ However, the NFE contingency plan was not updated to reflect the new disaster recovery site. In addition, the plan identified servers that were not in use. As a result, FDIC has limited assurance it will be able to efficiently implement continuity of operations for the NFE in the event of an emergency when knowledgeable employees are not available.

Conclusions

FDIC has made substantial progress in correcting previously reported weaknesses and has taken other steps to improve information security. Although five weaknesses from prior reports remain unresolved and new control weaknesses related to (1) e-mail security, (2) physical security, and (3) configuration management were identified, the remaining unresolved weaknesses previously reported and the newly identified weaknesses did not pose significant risk of misstatement in the corporation's financial statements for calendar year 2006. However, the old and new weaknesses do increase preventable risk to the corporation's financial and sensitive systems and information.

Since FDIC did not fully integrate its NFE into its information security program, it did not fully implement key control activities for NFE, such as sufficiently assessing risks, updating the security plan, reporting computer security incidents, or updating the contingency plan to reflect the current environment. Continued management commitment to integrating the NFE into the corporate information security program will be essential to ensure that the corporation's financial and sensitive information will be adequately protected. As the corporation continues to enhance the NFE, its reliance on controls implemented in this single, integrated financial system will increase. Until FDIC fully integrates NFE into the security

¹⁷In April of 2006, FDIC consolidated its disaster recovery capability into one disaster recovery site.

program, its ability to maintain adequate information system controls over its financial and sensitive information will be limited.

Recommendations for Executive Action

In order to sustain progress to its program, we recommend that the FDIC Chief Financial Officer and Chief Operating Officer direct that the following 12 actions be performed in a timely manner:

- Require that e-mail containing or transmitting accounting data be secured to protect the integrity of the accounting data.
- Train security personnel to implement the corporation's policy on physical security of the facility.
- Instruct FDIC personnel to lock rooms that contain sensitive software.
- Develop a configuration item index of all configuration items for NFE using a consistent and documented naming convention.
- Require that significant changes to the system, such as parameter changes, go through a formal change management process.
- Implement patches in a timely manner.
- Require that the NFE project team review status accounting reports and perform complete functional and physical configuration audits.
- Adequately control the NFE documents so that they are up-to-date and accurately reflect the current environment.
- Update the NFE risk assessment to include the risk associated with vulnerabilities identified during security testing and evaluation.
- Update the NFE security plan to clearly identify all common security controls.
- Develop procedures to review events occurring in the NFE to determine whether the events are computer security incidents.
- Update the contingency plan to reflect the new disaster recovery site and servers that are in use.

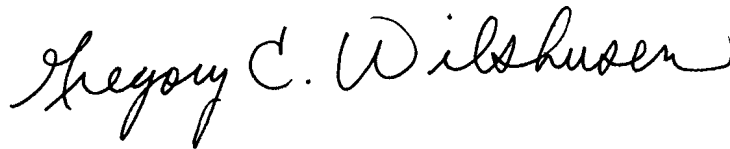
Agency Comments and Our Evaluation

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. II). The Deputy acknowledged the benefit of the recommendations made as part of this year's audit and stated that FDIC concurred with seven of our recommendations and has implemented or will implement them in the coming year. He also stated that FDIC partially concurred with our remaining five recommendations and has developed or implemented plans to adequately address the underlying risks that prompted these five recommendations, in some instances through alternative corrective actions.

With regard to the five recommendations to which FDIC partially concurred, if the corporation adequately implements the corrective actions below, it will have satisfied the intent of our recommendations. Regarding our recommendation that FDIC require that e-mail containing or transmitting accounting data be secured to protect the integrity of the accounting data, the Deputy stated that by July 31, 2007, FDIC will ensure that the integrity of accounting data transmitted by e-mail is appropriately protected, and that it will evaluate the various exchanges of accounting information and identify and document where more secure communications are needed. Concerning our recommendation that FDIC instruct personnel to lock rooms that contain sensitive software, the Deputy stated that FDIC has conducted additional analysis on the software that had access to payroll information and has removed that software from the desktop. With regard to our recommendation that FDIC require that significant changes to the system, such as parameter changes, go through a formal change management process, the Deputy stated that by December 31, 2007, FDIC will have developed procedures that will include appropriate management of, and documentation standards for, parameter changes. Based on the Deputy's comments, we have clarified our recommendation that FDIC update the NFE risk assessment to include the risk associated with vulnerabilities identified during security testing and evaluation. The Deputy stated that FDIC has since changed its process to require updates to the risk assessments when applications undergo major changes that affect the security of the system. Finally, with regard to the recommendation that FDIC develop procedures to review events occurring in the NFE to determine whether the events are computer security incidents, the Deputy stated that FDIC addressed this issue during the first quarter of 2007 when it established a formal process for monitoring and reviewing such events. In addition, FDIC plans to have documented procedures for elevating potential security violations to the incident handling team and for monitoring unusual events by August 31, 2007.

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 will also 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 III.

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive style with a large, prominent "G" and "W".

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Status of Previously Reported Weaknesses

| Weakness | Action completed | Action in progress |
|---|------------------|--------------------|
| Information Security: Information System Controls at the Federal Deposit Insurance Corporation (GAO-04-629) | | |
| Access authority | | |
| 1. Federal Deposit Insurance Corporation (FDIC) was using live data to support application development and testing. | X | |
| Network security | | |
| 2. Personal firewall settings for corporate examiner laptop computers that were used for remotely connecting to the network were not adequately secured. | X | |
| Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress (GAO-05-487SU) | | |
| Access controls | | |
| 3. Procedures were not established to prevent processes running in supervisor state in one logical partition from accessing datasets stored in another partition. | X | |
| 4. Procedures were not in place to identify and effectively control risks caused by sharing critical system components between production and nonproduction LPARs (logical partitions). | X | |
| Network security | | |
| 5. Structured query language database server configurations for many of FDIC's financial applications were not adequately secured. | X | |
| Application change control | | |
| 6. Procedures have not been consistently followed for authorizing, documenting, and reviewing all application software changes. | | X |
| Information Security: Federal Deposit Insurance Corporation Needs to Improve Its Program (GAO-06-619SU) | | |
| Access controls | | |
| 7. FDIC did not always change vendor-supplied account/password combinations. | X | |
| 8. FDIC did not adequately control inactive user accounts. FDIC policy requires accounts that have not been used within 60 days be deleted. | X | |
| 9. FDIC transmitted mainframe user and administrator passwords in plaintext across the network. | X | |
| 10. FDIC did not adequately enforce password management restrictions. | X | |
| Access rights and permissions | | |
| 11. FDIC access authorizations did not consistently support the access rights granted to New Financial Environment (NFE) users. | X | |
| 12. FDIC did not adequately control access to datasets containing sensitive data critical to the integrity of loss calculations used by the Division of Insurance. | X | |
| 13. FDIC did not effectively limit network access to sensitive personally identifiable and business proprietary information. | | X |

**Appendix I: Status of Previously
Reported Weaknesses**

Network services

| | |
|---|---|
| 14. FDIC did not securely configure Internet-accessible remote access to its information resources. | X |
| 15. FDIC permitted the use of unencrypted network protocols on its UNIX systems. | X |

Configuration assurance

| | |
|---|---|
| 16. FDIC did not securely configure an Oracle production database. | X |
| 17. FDIC did not properly secure the Apache Tomcat server that hosts a production database used by the employee time and attendance system. | X |
| 18. FDIC did not securely configure its workstations. | X |
| 19. FDIC laptop computers had unnecessary wireless technologies enabled. | X |
| 20. FDIC's Blackberry Enterprise Server and handheld devices were deployed and configured with several security weaknesses. | X |

Audit and monitoring of security-related events

| | |
|--|---|
| 21. FDIC did not effectively generate NFE audit reports or review them. | X |
| 22. FDIC's ability to monitor changes to critical mainframe datasets was inadequate. | X |
| 23. FDIC did not sufficiently audit system activities on its Oracle databases. | X |

Physical security

| | |
|--|---|
| 24. FDIC did not adequately control physical access to the Virginia Square computer processing facility. | X |
|--|---|

Segregation of duties

| | |
|--|---|
| 25. FDIC did not properly segregate incompatible system-related functions, duties, and capacities for an individual associated with the NFE. | X |
| 26. FDIC granted NFE accounts payable users inappropriate access to perform incompatible functions. | X |

Source: GAO.

Appendix II: Comments from the Federal Deposit Insurance Corporation



Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Deputy to the Chairman and CFO

April 25, 2007

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

Re: FDIC Management Response to the GAO 2006 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 Sustain Progress Improving Its Program, GAO-07-351. 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 2005, 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 2006.

We are pleased to accept GAO's acknowledgement of the substantial 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 twelve new recommendations to assist FDIC in sustaining the progress it has made enhancing its information security program. At this time, the FDIC concurs with seven recommendations and partially concurs with the remaining five. In instances where FDIC did not fully concur with specific GAO recommendations, FDIC has developed or implemented plans to adequately address the underlying risks that prompted the recommendations. In some instances, we chose to pursue alternative corrective actions. The detailed responses to these twelve new recommendations are provided in Attachment 1. Appendix I 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 the five, unresolved, 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

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

Mr. Gregory C. Wilshusen

- 2 -

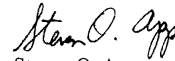
April 25, 2007

31, 2007. Corrective action for the remaining two will involve multi-year efforts to ensure a comprehensive solution. For those two multi-year efforts, the most significant risks will be addressed earlier in these projects wherever possible.

Once again, we thank you for your past contributions and your diligent work on this year's audit. We look forward to continuing our productive dialogue with the GAO as we continue to enhance our information security program.

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
Fred Selby
James H. Angel, Jr.
Audit Committee

FDIC Responses to GAO Recommendations
April 25, 2007

Recommendation 1: Require that e-mail containing or transmitting accounting data be secured to protect the integrity of the accounting data.

FDIC Response: Partially Concur

We agree that certain information may need additional security measures to protect the integrity of data transferred over an internal communication network. We disagree, however, with the specific example that e-mail containing or transmitting basic accounting information shared during the monthly New Financial Environment (NFE) closing process be secured beyond controls in the e-mail system. E-mail correspondence received/sent during the monthly process relating to accounting information used to produce journal entries such as the monthly expense accrual journal is between known parties, the normal monthly amount is known, and the data received is reviewed prior to being approved/recorded. This accounting data is reversed in the next period and does not impact in any way the amount that will eventually be paid to vendors. Any unusual information sent/received related to these journal entries would be followed up on prior to a journal entry being recorded in NFE. To ensure that the integrity of accounting data transmitted by e-mail is appropriately protected, the Division of Finance (DOF) will evaluate the various exchanges of accounting information within our business processes and identify and document where more secure communication methods are warranted. These actions will be completed by July 31, 2007.

Recommendation 2: That FDIC train security personnel to implement the corporation's policy on physical security of the facility.

FDIC Response: Concur

The Division of Administration (DOA) concurs with this recommendation. The DOA Security and Emergency Preparedness Section (SEPS) has implemented a physical security program that takes a proactive approach regarding facility access controls. The SEPS considers the security of FDIC personnel and protection of its facilities of utmost importance. Based on the GAO finding, the SEPS met with the FDIC's security guard contractor to discuss the situation. It was determined that the security breach was an isolated incident and, after an investigation was conducted, the Security Officer who allowed the unauthorized individual access to the FDIC facility was dismissed.

As part of the FDIC's Security Officer Orientation and Training, security officers are provided three days of intense on-the-job-training (OJT) to ensure that they are knowledgeable on all FDIC Security Policies and Procedures, post orders, general orders, special orders, and any other applicable security requirements. The OJT provides the awareness and working requirements that involve access control policies and procedures. In addition, as part of a SEPS long standing operating practice, a process exists whereby reminders are issued daily to all Security Officers that communicate the importance of enforcing all visitor access policies and procedures. The reminders are issued to security officers when the guards change shifts. SEPS will continue to ensure that incidents such as

FDIC Responses to GAO Recommendations
April 25, 2007

the reported security breach are addressed through the above cited training programs and daily guard briefings.

Recommendation 3: Instruct FDIC personnel to lock rooms that contain sensitive software.

FDIC Response: Partially Concur

The FDIC has taken very seriously the GAO statement of weakness in the draft report that, "a workstation that had access to a payroll system was located in an unsecured office. As a result, increased risk exists that unauthorized individuals could gain physical access to a key facility and to systems that have sensitive information." Accordingly, the FDIC immediately removed the questioned software from the desktop.

FDIC subsequently revisited GAO's concern by reviewing the security controls and potential vulnerabilities of the questioned software. Both the Division of Information Technology (DIT) Information Security and Privacy Staff and the Infrastructure Services Branch Server Engineering staff participated in this review.

- Based upon discussions with the GAO audit team, it was determined that GAO may have assumed that because this software was made available on a "limited use" basis, that the FDIC had concerns about the security of this software. In fact, the classification as "limited use" software by FDIC is a budgetary classification. The licenses for this software can be purchased on a desktop by desktop basis, which is more expensive per machine than FDIC's customary purchase of software on an enterprise basis but, nevertheless, can be very cost effective in instances where only a few individuals require access to the software. For budgetary reasons, FDIC decided to provide this software on a "limited use" basis, only as specifically required to perform critical business functions and where a less expensive alternative is not readily available.
- FDIC also understood from the GAO audit team that GAO may have had concerns that the software in question may be using an "unencrypted protocol" to facilitate "peer-to-peer" connections. The FDIC has evaluated this concern, and we believe that the proper encryption and authentication protocols were in place to mitigate these concerns.
- Finally, during the FDIC's discussion with the GAO audit team, it was confirmed that no connection to payroll or any other application was attempted or completed. The weakness statement in the GAO report indicates that, "...a workstation that had access to a payroll system was located in an unsecured office. As a result, increased risk exists that unauthorized individuals could gain physical access to a key facility and to systems that have sensitive information." This statement may lead some readers of this report to incorrectly believe that access was open to payroll data. FDIC maintains that the password and encryption controls FDIC had in place for this software properly restricts access and protects our corporate data.

In summary, FDIC's technical evaluation regarding the questioned software determined:

Attachment 1

FDIC Responses to GAO Recommendations
April 25, 2007

- The desktop software in question is not considered "Sensitive Software";
- The identified software itself does not introduce any additional risk to FDIC applications;
- Use of this software requires authentication to access the desktop and again to access the server;
- All traffic between the desktop software and the server is encrypted; and as a result
- Additional controls to physically lock offices are not required.

Recommendation 4: Develop a configuration item index of all configuration items for NFE using a consistent and documented naming convention.

FDIC Response: Concur

FDIC currently uses the following configuration management software to manage configuration changes:

- StarTeam is used to manage documentation and non-mainframe application source code.
- Endeavor is used to manage mainframe source code.
- PeopleSoft is used by the NFE project team for application development, and it includes its own internal configuration management capabilities.

Each of these tools can generate a listing of their managed configuration items on an ad-hoc basis that could potentially be used to develop the recommended item index using a documented naming convention. To ensure that FDIC implements an appropriate strategy for the development and maintenance of a complete listing of all configuration items and baseline configuration for NFE including application software, data files, software development tools, hardware and documentation, the FDIC will:

- review the current use of these configuration tools as well as other tools available; and
- make a determination regarding the best combination to be utilized to ensure the consistent implementation of configuration management controls for NFE.

Once this has been determined, the configuration item index and the document naming convention will be in place by December 31, 2007.

Recommendation 5: Require that significant changes to the system, such as parameter changes, go through a formal change management process.

FDIC Response: Partially Concur

Software changes already are required to go through a formal change control process. Although the parameter changes that resulted in this finding did not go through the formal change control process, these changes were coordinated with and the results reviewed by the necessary business areas. Not all changes need to go through the formal change control process; however, they

FDIC Responses to GAO Recommendations
April 25, 2007

should all be documented to support changes made. DOF is in the process of developing written procedures related to its systems operations and maintenance area which will include appropriate management of and documentation standards for parameter changes. Documentation will also be developed that defines which changes will go through a formal change control process and which ones will be covered by operating procedures. This action will be completed by December 31, 2007.

Recommendation 6: Implement patches in a timely manner.

FDIC Response: Concur

FDIC policy requires all high impact security and application software patches to be tested and implemented within a 14 day period, where practical. FDIC tests and approves all patches prior to installation in Production status. In practice some patches cannot be immediately deployed due to system or software incompatibility found during FDIC testing. This incompatibility results when patch updates cause any of the FDIC Production systems to perform improperly, making it impractical to install the particular patch within the 14 day window. A formal process to document and approve any required waivers to the patch installation policy was implemented April 15, 2004.

GAO correctly identified several Remote Client Network (RCN) servers upon which some security patch updates had not been installed in a timely manner. The RCN servers were located within the Demilitarized Zone (DMZ) of the FDIC protective firewall software. The DMZ protects the internal FDIC network by only allowing encrypted access to specific ports needed to access the service. FDIC employs two different software tools to perform automated scans on all servers to ensure all patches are installed and up to date. However, because access to the DMZ was blocked, the scan software did not detect that patches on the RCN servers were not up to date. Immediately upon notification by GAO, FDIC took corrective action to apply all missing patches to all RCN servers. Then, technical infrastructure engineers worked with the FDIC firewall support group to open ports so that patch updates can be pushed out to RCN servers and to include the RCN servers in periodic scan reports that identify missing patches. The scan reports are closely monitored and reconciled with related reports on the status of FDIC servers.

Recommendation 7: Require that the NFE project team review status accounting reports and perform complete functional and physical configuration audits.

FDIC Response: Concur

The FDIC recognizes the definitions of a Physical Configuration Audit and a Functional Configuration Audit provided by the Software Engineering Institute in its clarification regarding Specific Practices 3.2 in the Configuration Management Process Area. They are:

Attachment 1

FDIC Responses to GAO Recommendations
April 25, 2007

- “Physical configuration audits include the physical description that enables the reconstruction of products, product components, and baselines. This type of audit ensures the physical configuration is complete.”

As specified in the Configuration Management (CM) Plan, a physical configuration audit is conducted at the end of the Construction phase to ensure that Change Requests (CRs) targeted for the deployment are documented properly and that all artifacts changed against those CRs are correctly linked and labeled.

- “Functional configuration audits include the functional description that enables the evaluation of conformance to requirements. This type of audit ensures that the functional configuration is correct.”

The practice of Functional Configuration Audits is employed at the FDIC through the Rational Unified Process (RUP). The RUP process specifies that the application be tested through a formal process to determine if the changes made to the application are consistent with the requirements specified in the Inception Phase. The testing process in the Construction and Transition RUP phases results in a Test Analysis Report, which serves as the documentation that the application’s “as-tested” functional characteristics are in conformance with the “as-specified” characteristics. This process is performed by the project team each time there is a change to the application and is documented through the RUP artifacts and stored in StarTeam. Additional guidance regarding audits is provided in the CM Plan.

Status Accounting reports contain the information needed to manage software configuration items effectively (i.e., status of proposed changes or the implementation status of approved changes to the baselines) and are used to support configuration auditing. StarTeam provides a reporting capability for ad-hoc charts and reports. The two most common reports are the Change Request Link Report and a listing of artifacts based on View Label. The NFE Project Team is currently using these reports, though not necessarily storing the output. A process change will be implemented to ensure that these artifacts are maintained in the NFE StarTeam project.

The CM Plan will be updated, and FDIC will complete physical and functional audits and status accounting reports (as defined in our response) by December 31, 2007.

Recommendation 8: Adequately control the NFE documents so that they are up-to-date and accurately reflect the current environment.

FDIC Response: Concur

The FDIC has implemented the Certification and Accreditation program, which provides a timely methodology and process for maintaining the key primary documentation noted by the

FDIC Responses to GAO Recommendations
April 25, 2007

GAO audit team. The FDIC had already scheduled updates to the Security Test and Evaluation and Certification and Accreditation (C&A) reviews for NFE to be performed during 2007. The C&A is intended to address changes in the NFE environment that will also address GAO residual concerns with FDIC's use of the more detailed and robust draft of NIST 800-53 controls in the initial C&A review process. The final C&A package will include updated C&A artifacts as appropriate. The NFE business owner, supported by DIT Information Security and Privacy Staff, will monitor the C&A package to ensure that it incorporates all major modifications and changes since the prior C&A that was completed during 2005. The above C&A tasks will be completed by December 31, 2007.

To further ensure that future changes are properly captured and maintained, the DIT NFE project manager in coordination with the DOF Information Security Manager and DIT ISPS will manage the configuration of each of these documents in StarTeam. The documents will be updated at the points called for by the FDIC RUP SDLC, and reviewed at the milestones called for by the FDIC RUP. This process will be established by June 30, 2007.

Recommendation 9: Update the NFE risk assessment to include the identified vulnerabilities in security testing and evaluation.

FDIC Response: Partially Concur

FDIC agrees with the overriding principle that we believe is behind this recommendation, which is that identified risks and open vulnerabilities should be properly identified and brought to the attention of the certifying and accrediting officials in the risk management process. However, the FDIC does not agree with the recommendation as specifically written. The Risk Assessment is a judgmental examination of the probability of potential harmful events conducted early in the development process by internal FDIC staff and is not an appropriate place to capture results from the independent Security Testing and Evaluation (ST&E) review or other processes. In the FDIC's current process, vulnerabilities or security control weaknesses detected during the ST&E or other independent processes are assigned a risk rating by an independent team and are tracked in a Plan of Actions and Milestones (POA&M).

The POA&M is the document that should be updated throughout the risk management process in order to track and mitigate vulnerabilities. Through the ST&E portion of the risk management process, security control weaknesses are independently identified and rated with an appropriate risk level. Within the RUP, the FDIC already requires updates to risk assessments when applications undergo major changes that affect the security posture of the system or application.

Vulnerabilities that are mitigated in the POA&M are independently verified or retested, as appropriate, by an independent team within the DIT Information Security and Privacy Staff to confirm closure. Remaining vulnerabilities for which risk is accepted are documented in an acceptance of risk (AOR) form that is made part of the documentation that is provided to the Certifying Official as part of the Certification and Accreditation process. The Certifying Official

FDIC Responses to GAO Recommendations
April 25, 2007

looks at any remaining open items on the POA&M that have mitigation plans and at the risks being accepted in the AOR and uses them to prepare a Security Assessment Report (SAR) that is provided along with all the other C&A documentation to the Accreditation Official for consideration during the accreditation decision. Based upon the Accreditation Official's assessment, the system is either given full Authority to Operate (ATO) or given an Interim Authority to Operate (IATO). This process, as documented above, is in place now, but was not fully in place at the time of the GAO's audit; therefore, this change represents an improvement that we expect the GAO will be able to observe and verify upon subsequent re-test. We believe that the actions we have already taken are fully responsive to this recommendation.

Recommendation 10: Update the NFE security plan to clearly identify all common security controls.

FDIC Response: Concur

The FDIC concurs that, at the time of the audit, the NFE security plan was out of date. FDIC believes that this is partially a timing issue in the documentation due to the effort already underway in FDIC to identify and incorporate common security controls into the recently implemented revised security plan templates. The FDIC has developed a new Security Plan Template, and is updating the NFE Security Plan to conform to this template which we believe will bring the plan in line with NIST 800-18 requirements and NIST 800-53 controls. By May 31, 2007, FDIC will update the NFE Security Plan to include information about FDIC's common controls as well as a reference to the document that contains the correct server and mainframe hardware information.

Recommendation 11: Develop procedures to review events occurring in the NFE to determine whether the events are computer security incidents.

FDIC Response: Partially Concur

As GAO is aware, FDIC is in the process of enhancing report monitoring and evaluating additional options for audit logging for NFE. We believe the match exception override example cited should be incorporated into report monitoring and/or audit logging findings rather than raised as if it is a separate and distinct finding. That said, we concur with the GAO that at the time of its review we did not have formal procedures to review match exception overrides performed by the Disbursements Unit staff. This supervisory review issue was addressed during the first quarter of 2007 when we established a more formal process for monitoring and reviewing these events. A match override report was created and is now being reviewed and approved weekly by the supervisor of the Disbursement Operations Unit. To address GAO's broader recommendation of reviewing system events, the FDIC will document procedures for elevating potential security violations to CSIRT and for monitoring unusual/unexpected events

Attachment 1

FDIC Responses to GAO Recommendations
April 25, 2007

as identified by our current audit logging, audit triggers/alerts, and program monitoring efforts. Procedures will be developed by August 31, 2007.

Recommendation 12: Update the contingency plan to reflect the new disaster recovery site and servers that are in use.

Response: Concur

The NFE contingency plan was updated March 29, 2007, to reflect the new disaster recovery site and to include an updated list of servers that are in use to ensure continuity of operations in the event of a disaster. The corrective actions taken in response to this recommendation have been completed.

FDIC Responses to Unresolved Prior Year Weaknesses
April 25, 2007

As noted in GAO's draft report, the FDIC has corrected or mitigated 21 of the 26 weaknesses that GAO previously identified as unresolved at the completion of its 2005 audit. Also noted in this report is that actions are in progress for the remaining five. The status of each of these five is discussed below. The numbers correspond to the numbers used by GAO in its report.

Application Change Control

Weakness 6: Procedures have not been consistently followed for authorizing, documenting, and reviewing all application software changes.

Status: FDIC has included our response to this weakness in Attachment 1, FDIC Responses to GAO Recommendations, as part of our response to GAO recommendations #4, #7, and #8.

Access Rights and Permissions

Weakness 13: FDIC did not effectively limit network access to sensitive, personally identifiable and business proprietary information.

Status: The FDIC launched a formal project to address this issue and will monitor progress under a 2007 Corporate Goal. An executive sponsor for the project has been selected, and a project work plan has been developed. The Work Plan establishes the FDIC commitment to identify FDIC network shared storage sites that contain sensitive, personally identifiable and business proprietary information. This will be a multi-year project, and the completion date is to be determined in conjunction with completion of the initial tasks.

Auditing and Monitoring of Security-Related Events

Weakness 21: FDIC did not effectively generate NFE audit reports or review them.

Status: In our follow-up action response memo to GAO of November 15, 2006, we agreed that addressing this recommendation may provide an opportunity to further strengthen the FDIC's control environment, and we identified many logging/trigger/analytics to be pursued. However, we do not concur that all controls must be built into the system itself and would point out that management's assessment of controls appropriately takes into account the entire control environment, both automated and manual. We are evaluating and developing event triggers/monitoring reports where current capabilities of financial activity traceability in the system exist. In addition, if key components of traceability are not available in the system transaction logs, then FDIC will evaluate, in conjunction with the NFE upgrade, the costs and benefits of expanding system logging capabilities versus utilizing other analytical tools and techniques to minimize the risk of unauthorized financial transaction processing. The target completion date for developing key items identified in the November 2006 response that can be addressed within current system capabilities is December 31, 2007.

FDIC Responses to Unresolved Prior Year Weaknesses
April 25, 2007

Physical Security

Weakness 24: FDIC did not adequately control physical access to the Virginia Square computer processing facility.

Status: FDIC has completed steps to more tightly control physical access to the Virginia Square computer facility (Data Center) including the following:

- developed Data Center access reports to provide an automated reporting tool to monitor access to the Data Center;
- updated the Data Access Control procedure to include “executive privilege” clause; and
- implemented new door groupings.

FDIC is currently in the process of:

- reauthorizing Data Center Access Forms; and
- entering the updated information into the FDIC physical access control system.

Final actions are planned for completion by June 30, 2007.

Segregation of Duties

Weakness 25: FDIC did not properly segregate incompatible system-related functions, duties, and capacities for an individual associated with the NFE.

Status: FDIC completed actions to address incompatible duties associated with the individual identified by GAO. In addition, to ensure that incompatible roles do not exist under other circumstances, the Division of Finance initiated a project to restructure NFE security. The goal of this project is to conduct a comprehensive analysis of current NFE security and business requirements in order to develop a recommendation for a role-based security design that will reconfigure the current NFE security to ensure that appropriate access is granted to all users of NFE. It will encompass best practices, including separation of duties. Additionally, the NFE Security Restructuring project will provide the FDIC with a system security solution that is easily maintained and more easily understood by business owners, managers, and DOF security personnel. The project is risk-based with higher priority assigned to reviewing riskier areas at the beginning of the project. If any significant weaknesses are identified during the project, they will be addressed timely. Significant weaknesses will be documented and resolved in one of several ways: as part of the project, through a system change request, or through security maintenance. Compensating controls, as appropriate to mitigate risk, will be put in place until resolution. The project will culminate with a change to role-based security and is scheduled to be completed by July 31, 2008.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov

Staff Acknowledgments

In addition to the individual named above, William F. Wadsworth, Assistant Director; Verginie A. Amirkhanian; Daniel D. Castro; Patrick R. Dugan; Edward Glagola Jr.; Mickie E. Gray; David B. Hayes; Kaelin P. Kuhn; Duc M. Ngo; Tammi L. Nguyen; Eugene E. Stevens IV; Henry I. Sutanto; and Amos Tevelow 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 "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