

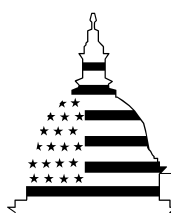
GAO

Report to the Board of Directors, Federal
Deposit Insurance Corporation

May 2005

INFORMATION
SECURITY

Federal Deposit
Insurance Corporation
Needs to Sustain
Progress



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-05-486](#), a report to the Board of Directors, Federal Deposit Insurance Corporation

Why GAO Did This Study

The Federal Deposit Insurance Corporation (FDIC) relies extensively on computerized systems to support its financial and mission-related operations. As part of GAO's audit of the calendar year 2004 financial statements for the three funds administered by FDIC, GAO assessed (1) the progress FDIC has made in correcting or mitigating information system control weaknesses identified in our audits for calendar years 2002 and 2003 and (2) the effectiveness of the corporation's information system general controls.

What GAO Recommends

To improve information system controls, GAO recommends that the FDIC Chairman direct the Chief Information Officer to implement an ongoing, comprehensive process of tests and evaluations to ensure that all key control areas supporting FDIC's financial environment are routinely reviewed and tested. In commenting on a draft of this report, FDIC agreed with our recommendations. FDIC plans to address the identified weaknesses and indicated that significant progress has already been made.

www.gao.gov/cgi-bin/getrpt?GAO-05-486.

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 wilshusen@gao.gov.

INFORMATION SECURITY

Federal Deposit Insurance Corporation Needs to Sustain Progress

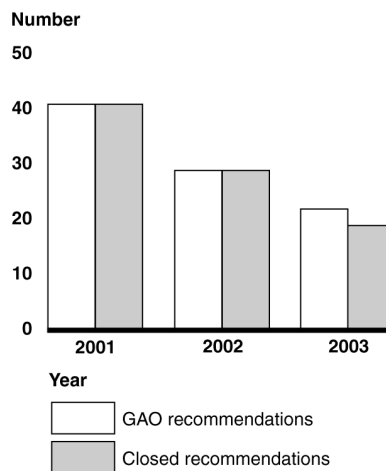
What GAO Found

FDIC has made significant progress in correcting previously reported information system control weaknesses and has taken other steps to improve information security. Of the 22 weaknesses reported in GAO's 2003 audit, FDIC corrected 19 and is taking action to resolve the 3 that remain. In addition, it corrected the one weakness still open from GAO's 2002 audits (see figure).

Although FDIC has made substantial improvements in its information system controls, GAO identified additional weaknesses that diminish FDIC's ability to effectively protect the integrity, confidentiality, and availability of its financial and sensitive information systems. These included weaknesses in electronic access controls, network security, segregation of computer functions, physical security, and application change control. Although these do not pose significant risks to FDIC's financial and sensitive systems, they warrant management's action to decrease the risk of unauthorized modification of data and programs, inappropriate disclosure of sensitive information, or disruption of critical operations.

A key reason for FDIC's weaknesses in information system controls is that it had not fully implemented a complete test and evaluation process, which is a key element of a comprehensive agency information security program with effective controls. Although FDIC has made substantial progress in implementing its information security program and has enhanced its process to test and evaluate its information system controls, it did not ensure that all key control areas supporting FDIC's financial environment are routinely reviewed and tested. These control areas included electronic access, network security, and audit logging.

FDIC Progress in Implementing GAO Recommendations



Source: GAO.

Contents

Letter

	1
Results in Brief	2
Background	3
Objectives, Scope, and Methodology	4
FDIC Has Made Significant Progress in Correcting Weaknesses and Implementing Controls	6
Weaknesses in Information System Controls	7
FDIC Has Made Substantial Progress Implementing Information Security Program but Has Not Completed Key Element	11
Conclusions	13
Recommendation for Executive Action	14
Agency Comments	14

Appendixes

Appendix I: Comments from the Federal Deposit Insurance Corporation	16
Appendix II: GAO Contact and Staff Acknowledgments	18

Abbreviations

CIO	Chief Information Officer
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Management Act
FISCAM	Federal Information System Controls Audit Manual
FSLIC	Federal Savings and Loan Insurance Corporation
NIST	National Institute of Standards and Technology

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, D.C. 20548

May 19, 2005

To the Board of Directors
Federal Deposit Insurance Corporation

Effective information system controls are essential to ensuring that financial information is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction. These controls also affect the integrity, confidentiality, and availability of nonfinancial information maintained by Federal Deposit Insurance Corporation (FDIC), such as personnel and bank examination information.

As part of our audit of the calendar year 2004 financial statements for FDIC's Bank Insurance Fund, Savings Association Fund, and FSLIC (Federal Savings and Loan Insurance Corporation) Resolution Fund,¹ we assessed (1) the progress FDIC has made in correcting or mitigating information system control weaknesses reported in our prior audits for calendar years 2002² and 2003³ and (2) the effectiveness of the corporation's information system general controls.⁴ In a separate report designated for "Limited Official Use Only," we are making recommendations to correct the specific weaknesses identified.

We performed our review at FDIC headquarters in Washington, D.C., and its computer facility in Arlington, Virginia, from September 2004 through February 2005. Our review was performed in accordance with generally accepted government auditing standards.

¹GAO, *Financial Audit: Federal Deposit Insurance Corporation Funds' 2004 and 2003 Financial Statements*, [GAO-05-281](#) (Washington, D.C.: Feb. 11, 2005).

²GAO, *Information Security: Improvements Made but Existing Weaknesses Place Data at Risk*, [GAO-03-630](#) (Washington, D.C.: June 18, 2003).

³GAO, *FDIC Information Security: Information System Controls at the Federal Deposit Insurance Corporation*, [GAO-04-630](#) (Washington, D.C.: May 28, 2004).

⁴Information 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 protection designed to ensure that access to data is appropriately restricted, that only authorized changes to computer programs are made, that computer security duties are segregated, and that backup and recovery plans are adequate to ensure the continuity of operations.

Results in Brief

FDIC made significant progress in correcting previously reported information system control weaknesses and has taken other steps to improve information security. Of the 22 weaknesses reported in our 2003 audit, FDIC corrected 19 and is taking action to resolve the 3 that remain. In addition, it corrected the one weakness still open from our 2002 review.

Although FDIC has made substantial improvements in its information system controls, GAO identified additional weaknesses that diminish FDIC's ability to effectively protect the integrity, confidentiality, and availability of its financial and sensitive information systems. These included weaknesses in electronic access controls, network security, segregation of computer functions, physical security, and application change control. Although these do not pose significant risks to FDIC's financial and sensitive systems, they warrant management's action to decrease the risk of unauthorized modification of data and programs, inappropriate disclosure of sensitive information, or disruption of critical operations.

A key reason for FDIC's weaknesses in information system controls is that it had not fully implemented a complete test and evaluation process, which is a key element of a comprehensive agency information security program. Although FDIC has made substantial progress in implementing its information security program and has enhanced its process to test and evaluate its information system controls, it did not ensure that all key control areas supporting FDIC's financial environment were routinely reviewed and tested. This included areas such as electronic access, network security, and audit logging. Without routine tests and evaluations of all key information system control areas, FDIC's ability to maintain adequate information system controls over its financial and sensitive information will be limited.

We are recommending that FDIC broaden its process of tests and evaluations to ensure that all key control areas supporting its financial environment are routinely reviewed and tested.

In providing written comments on a draft of this report, FDIC's Chief Financial Officer agreed with our recommendations. He reported that FDIC plans to address the identified weaknesses and that significant progress has already been made.

Background

Congress created FDIC in 1933⁵ 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.⁶ The act created the Bank Insurance Fund and the Savings Association Insurance Fund, both of which are responsible for protecting insured bank and thrift depositors. The act 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. It also designated FDIC as the administrator of these funds. As part of this function, FDIC has an examination and supervision program to monitor the safety of deposits held in member institutions.

FDIC insures deposits in excess of \$10 trillion for about 8,900 institutions. Together, the three funds—the Bank Insurance Fund, the Savings Association Insurance Fund, and the FSLIC Resolution Fund—have about \$52 billion in assets. FDIC had a budget of about \$1.1 billion for calendar year 2004 to support its activities in managing the three funds. For that year, it processed more than 3.8 million financial transactions.

FDIC 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, it 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, about 6,200 individuals were authorized to use FDIC's systems. The corporation's key official for computer security is the Chief Information Officer, who is responsible for establishing, implementing, and overseeing a corporatewide information security program.

Information system controls are a critical consideration for any organization that depends on computerized systems and networks to carry

⁵Federal Deposit Insurance Corporation Act, June 16, 1933, Ch. 89, § 8.

⁶Pub. L. No. 101-73 (Aug. 9, 1989).

out its mission or business. Without proper safeguards, there is risk that individuals and groups with malicious intent may intrude into inadequately protected systems and use this access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

We have reported information security as a governmentwide high-risk area since February 1997.⁷ Our previous reports, and those of agency inspectors general, describe persistent information security weaknesses that place a variety of federal operations, including those at FDIC, at risk of disruption, fraud, and inappropriate disclosure.

Congress and the executive branch have taken action to address the risks associated with persistent information security weaknesses. In December 2002, the Federal Information Security Management Act (FISMA) of 2002, which is intended to strengthen information security, was enacted as Title III of the E-Government Act of 2002.⁸ In addition, the administration undertook important actions to improve security, such as integrating information security into the *President's Management Agenda Scorecard*. Moreover, the Office of Management and Budget and the National Institute of Standards and Technology (NIST) have issued information security guidance to agencies.

Objectives, Scope, and Methodology

The objectives of our review were to assess (1) the progress FDIC had made in correcting or mitigating weaknesses reported in connection with our financial statement audits for calendar years 2002⁹ and 2003¹⁰ and (2) the effectiveness of the corporation's information system controls. Our evaluation was based on (1) our *Federal Information System Controls Audit Manual* (FISCAM),¹¹ which contains guidance for reviewing information system controls that affect the integrity, confidentiality, and

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

⁸Pub. L. No. 107-347 (Dec. 17, 2002).

⁹[GAO-03-630](#).

¹⁰[GAO-04-630](#).

¹¹GAO, *Federal Information System Controls Audit Manual, Volume I—Financial Statements Audits*, [GAO/AIMD-12.19.6](#) (Washington, D.C.: January 1999).

availability of computerized data and (2) our May 1998 report on security management best practices¹² at leading organizations, which identifies key elements of an effective information security program.

Specifically, we evaluated information system controls intended to

- prevent, limit, and detect electronic 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 espionage, sabotage, damage, and theft;
- ensure that work responsibilities for computer functions are segregated so that no one individual controls all key aspects of a computer-related operation and thereby has the ability to conduct unauthorized actions or gain unauthorized access to assets or records without detection by another individual performing assigned responsibilities;
- prevent the implementation of unauthorized changes to application or system software;
- ensure recovery of computer process operations and data in case of disaster or other unexpected interruption; and
- ensure an adequate information security program.

To evaluate these controls, we identified and reviewed pertinent FDIC security policies and procedures, guidance, plans, and reports. We also discussed whether information system controls were in place, adequately designed, and operating effectively with key security representatives, system administrators, and management officials. In addition, we conducted tests and observations of controls in operation and reviewed corrective actions taken by the corporation to address vulnerabilities identified in our audits for calendar years 2002¹³ and 2003.¹⁴

¹²GAO, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

¹³GAO-03-630.

¹⁴GAO-04-630.

FDIC Has Made Significant Progress in Correcting Weaknesses and Implementing Controls

FDIC has made significant progress in correcting previously reported information system control weaknesses. Of the 22 weaknesses reported in our 2003 audit,¹⁵ FDIC corrected 19 and is taking action to resolve the 3 that remain. In addition, the corporation corrected the one¹⁶ weakness still open from our 2002 audit.¹⁷ FDIC's actions included resolving weaknesses related to its key access controls, network security, and monitoring capabilities. For example, the corporation

- restricted user access to critical financial and sensitive data and programs;
- strengthened security configurations of network devices, including firewalls, routers, switches, and servers; and
- enhanced its monitoring of security-relevant events by fully implementing its intrusion detection system to monitor its computer network traffic for unusual or suspicious access activities.

In addition to addressing previously reported weaknesses, FDIC took other steps to improve information security. For example, the corporation strengthened its oversight of contractor connections to its network by requiring contractors to develop security plans to protect these connections and to perform periodic inspections of contractor facilities to ensure security effectiveness. Further, FDIC established certification and accreditation¹⁸ guidelines that outline requirements for performing this process as part of each system's life cycle and certified and accredited each of its key systems. In addition, the corporation updated its disaster

¹⁵[GAO-04-630](#).

¹⁶GAO identified 29 weaknesses in the 2002 review; FDIC corrected 28 of those weaknesses before our 2004 review. In addition, GAO identified 41 weaknesses in the 2001 review that were also corrected before our 2004 review.

¹⁷[GAO-03-630](#).

¹⁸Certification is the comprehensive evaluation of the management, operational, technical, and security controls in an information system to determine the effectiveness of these controls and identify existing vulnerabilities. Accreditation is the official management decision to authorize operation of an information system. This authorization explicitly accepts the risk remaining after the implementation of an agreed-upon set of security controls.

recovery procedures and has been routinely performing different types of tests of its disaster recovery plan.

Weaknesses in Information System Controls

Although FDIC made substantial improvements in its information system controls, we identified 20 additional weaknesses that diminish its ability to effectively protect the integrity, confidentiality, and availability of its financial and sensitive information and information systems. Specifically, we identified weaknesses in electronic access controls, network security, physical security, segregation of computer functions, and application change controls. Although these information system control weaknesses do not pose significant risks to FDIC's financial and sensitive systems, they warrant management's action to decrease the risk of unauthorized modification of data and programs, inappropriate disclosure of sensitive information, or disruption of critical operations.

Electronic Access Controls

A basic management control objective for any organization is the protection of its information systems and critical data from unauthorized access. Organizations accomplish this objective by granting employees the authority to read, create, or modify only those programs and data that they need to perform their duties. Effective electronic access controls should be designed to restrict access to computer programs and data and detect unauthorized access. These controls include assigning user access rights and permissions and reviewing audit logs to ensure that access privileges are used appropriately.

Although FDIC restricted access to programs and information, we found instances in which access was not sufficiently controlled. For example, about 250 users were inadvertently granted access to read, create, or modify critical production programs and data for financial, payroll/personnel, and bank regulatory systems. The risk of weakening security access was further heightened because the access activities of these users were not being logged for review. In addition, emergency access accounts with broad system access to all critical system and security resources intended to be used solely to manage problems or emergencies that interrupt the system's 24-hour-a-day operation were routinely used by four system and operations staff. Further, FDIC did not configure security software to appropriately restrict, log, and monitor access to certain sensitive system software libraries. As a result, increased risk exists that individuals could circumvent security controls to read,

create, or modify critical or sensitive programs and data, possibly without detection.

In response to these weaknesses, FDIC's Chief Information Officer said that they have taken steps to restrict access to critical financial data and program and related sensitive information. Further, the corporation stated that it has restricted access to sensitive system software libraries and plans to generate monthly audit reports for review and follow-up action as needed.

Network Security

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. 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. Network devices include (1) firewalls designed to prevent unauthorized access to and from the network, (2) routers that filter and forward data along the network, (3) switches that forward information among parts of a network, and (4) servers that host applications and data. Network services consist of protocols for transmitting data between network devices. In addition, effective network controls, such as passwords, should be established to authenticate authorized users who access the network from local and remote locations. Since networks often provide the entry point for access to electronic information assets, failure to secure them increases the risk of unauthorized use of sensitive data and systems.

Although FDIC's network controls were generally effective, we identified instances where FDIC did not adequately secure specific network services and devices or protect passwords. For example, database server configurations for some of the corporation's financial applications were not adequately secured. These servers had insecure settings that could have allowed an unauthorized user to gain access without providing authentication. In addition, FDIC did not have controls in place to consistently ensure that data transmitted between network devices were secure. Further, the passwords of local network administrators who had broad system access privileges were not adequately secured. As a result, increased risk exists that a malicious user could gain unauthorized access

to some of FDIC's sensitive network systems, read and modify sensitive system data, and disrupt or deny computer processing services to corporation employees.

In response to these weaknesses, FDIC's Chief Information Officer said that the corporation had taken steps to improve network security including strengthening server settings, data transmission, and administrator passwords.

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 by periodically reviewing access rights granted to ensure that access continues to be appropriate based on criteria established for granting it. At FDIC, physical access control measures (such as guards, badges, and locks, used either alone or in combination) are vital to protecting computing resources and the sensitive data it processes from external and internal threats.

Although FDIC had taken numerous actions to strengthen its physical security over its computing environment, certain weaknesses reduced its effectiveness in protecting and controlling physical access to sensitive work areas. For example, 4 employees and contractors had access to the computer data center even though they had changed their job responsibilities and no longer required this access. As a result, there is an increased risk that unauthorized individuals could gain access to sensitive computing resources and data and inadvertently or deliberately misuse or destroy them.

In response, FDIC's management plans to update procedures to ensure that physical access to the data center is limited to authorized individuals.

Segregation of Computer Functions

Segregation of computer functions refers to the policies, procedures, and organizational structure that helps ensure that one individual cannot independently control all key aspects of a process or computer-related operation and, thereby, gain unauthorized access to assets or records. Often segregation of computer functions is achieved by dividing responsibilities among two or more organizational groups. Dividing duties among two or more individuals or groups diminishes the likelihood that

errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the others. Inadequate segregation of computer functions increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed.

Although computer responsibilities were generally properly segregated at FDIC, we identified one instance in which responsibilities were not adequately segregated: system administrators were also serving as database administrators for systems that maintained FDIC's key financial information. The risk associated with this weakness was further heightened because these administrators could take full control over the financial applications and databases that include audit and reconciliation data. Consequently, there is an increased risk that these individuals could perform unauthorized system activities without being detected.

In response to this weakness, FDIC's Chief Information Officer said that the corporation plans to segregate the duties of system and database administrator functions.

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 needed, work as intended, and do not result in the loss of data or program integrity, such changes should be authorized, tested, and independently reviewed.

Although FDIC had application change control procedures for its general ledger and accounts payable mainframe applications, it did not have procedures for documenting tests performed or independent reviews made for changes made to other key mainframe and client/server financial applications. In addition, the corporation did not have a process for authorizing changes to Web-based financial applications. Without adequate application change control procedures, changes may be implemented that are not authorized, tested, or independently reviewed.

In response, FDIC's Chief Information Officer plans to establish procedures for documenting tests performed and independent reviews made for application software changes made to all mainframe and client/server application software. In addition, the corporation plans to establish a process for authorizing changes to Web-based financial applications.

FDIC Has Made Substantial Progress Implementing Information Security Program but Has Not Completed Key Element

A key reason for FDIC's weaknesses in information system controls is that it had not fully implemented a complete test and evaluation process, which is a key element of a comprehensive agency information security program. Our May 1998 study¹⁹ of security management best practices determined that a comprehensive information security program is essential to ensuring that information system controls work effectively on a continuing basis. Also, FISMA,²⁰ consistent with our study, requires an agency's information security program to include certain key elements. These elements include

- a central information security management structure to provide overall security policy and guidance along with oversight to ensure compliance with established policies and reviews of the effectiveness of the information security environment;
- periodic assessments of the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;
- policies and procedures that (1) are based on risk assessments, (2) cost effectively reduce risks, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- security awareness training to inform personnel, including contractors and other users of information systems, of information security risks and their responsibilities in complying with agency policies and procedures; and
- a process of tests and evaluations of the effectiveness of information security policies, procedures, and practices relating to management, operational, and technical controls of every major information system identified in the agency's inventories.

¹⁹GAO/AIMD-98-68.

²⁰FISMA 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 has made substantial progress in establishing a comprehensive information security program. The corporation strengthened its central information security management structure by providing additional staff resources to oversee the program. Further, the corporation initiated a program to routinely perform risk assessments on all major systems. In addition, FDIC updated its overall security policies covering network security, computer center access, and security management and it developed security plans for all key systems. Also, the corporation continued to enhance its security awareness program by adding specialized training for selected technical staff.

Although FDIC enhanced its process to test and evaluate its information system controls, it did not ensure that all key control areas supporting the corporation's financial environment were routinely reviewed and tested. These areas included electronic access controls, network security, and audit logging. During the past year, FDIC strengthened its test and evaluation process to cover additional key information system control areas, provide for independent tests of corrective actions, and assess and test newly-identified weaknesses and emerging security threats. Although FDIC established a process to test and evaluate network and mainframe information system controls, its program did not include routine evaluations of network desktop and database application controls. Further, the process did not include comprehensive tests to ensure that electronic access to key financial programs and data (1) were restricted to only those users who need it to perform their job functions and (2) had appropriate audit logs maintained to record security-relevant events for subsequent review. Without routine tests and evaluations of all key information system control areas, FDIC will have limited assurance that its financial and sensitive information is adequately protected.

Incorporating these key areas into its test and evaluation process should allow FDIC to better identify and correct security problems, such as those identified in our 2004 audit. Further, the corporation's implementation of new financial systems in the coming year will significantly change the nature of its information systems environment and of the related information systems controls necessary for their effective operation. Consequently, a comprehensive test and evaluation process that includes these areas will be essential to ensure that the corporation's financial and sensitive information will be adequately protected in this new environment.

In response, FDIC's Chief Information Officer said that the corporation will continue to take steps to enhance its overall test and evaluation process to ensure an effective security environment.

Conclusions

FDIC has made significant progress in correcting the information system control weaknesses we previously identified and has taken other steps to improve information security. Although we identified weaknesses in information system controls involving electronic access, network security, segregation of computer functions, physical security, and application change control, these weaknesses do not pose significant risks to FDIC's financial and sensitive systems. Accordingly, we concluded that weaknesses in information system controls at the corporation no longer constitute a reportable condition,²¹ as stated in our audit of the calendar year 2004 financial statements for FDIC's three funds.²² However, they warrant action by the FDIC management to decrease the risk of unauthorized modification of data and programs, inappropriate disclosure of sensitive information, or disruption of critical operations.

A key reason for FDIC's weaknesses in information system controls is that it had not fully implemented a complete test and evaluation process, which is a key element of a comprehensive agency information security program. Although the corporation has made substantial progress in implementing its information security program and enhanced its process to test and evaluate its information system controls, it did not ensure that all key control areas supporting its financial environment were routinely reviewed and tested. These areas included electronic access controls, network security, and audit logging. Until FDIC fully implements a comprehensive test and evaluation process, its ability to maintain adequate information system controls over its financial and sensitive information will be limited. This will be especially crucial as the corporation implements new financial systems in the coming year.

²¹Reportable conditions involve matters coming to the auditor's attention that, in the auditor's judgment, should be communicated because they represent significant deficiencies in the design or operation of internal control and could adversely affect FDIC's ability to meet the control objectives.

²²GAO-05-281.

Recommendation for Executive Action

To strengthen FDIC's information security program, we recommend that the Chairman direct the Chief Information Officer to broaden its process of tests and evaluations to ensure that all key control areas supporting FDIC's financial environment are routinely reviewed and tested. This process should include routine tests and evaluations of key control areas such as electronic access, network security, and audit logging.

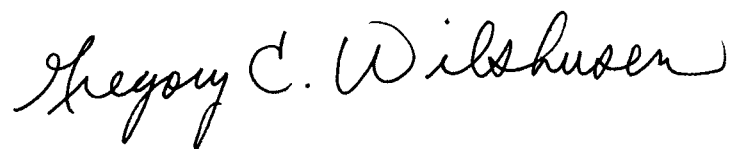
We are also making recommendations in a separate report designated for "Limited Official Use Only." These recommendations address actions needed to correct specific information security weaknesses related to electronic access, network security, physical security, segregation of computer functions, and application change controls.

Agency Comments

In providing written comments on a draft of this report, FDIC's Chief Financial Officer (CFO) agreed with our recommendations. His comments are reprinted in appendix I of this report. Specifically, FDIC plans to correct all weaknesses identified and broaden the testing and evaluation element of its computer management program by February 28, 2006. According to the CFO, significant progress has already been made in addressing the identified weaknesses.

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 David W. Irvin, Assistant Director, at (214) 777-5716. We can also be reached by e-mail at wilshuseng@gao.gov and irvind@gao.gov, respectively. Key contributors to this report are listed in appendix II.

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

Comments from the Federal Deposit Insurance Corporation



Federal Deposit Insurance Corporation
550 17th Street, NW, Washington, DC 20429

Deputy to the Chairman and Chief Financial Officer

May 9, 2005

Mr. Gregory C. Wilshusen, Director
Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to respond to the draft reports entitled, Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress, dated April 26, 2005. We appreciate the generally positive tone of these reports, particularly in the Government Accountability Office's (GAO's) acknowledgement of the significant improvements made and the lengthy discussion of a number of the internal controls we have implemented. We were also pleased to have GAO acknowledge that, although the weaknesses identified warrant attention, they do not pose significant risks to FDIC's financial and sensitive systems.

While recognizing that FDIC has made significant progress in correcting the prior year information security weaknesses and has taken other steps to improve security, GAO did identify new internal control matters. These weaknesses were characterized as being the result of FDIC not having a complete test and evaluation process. We appreciate the detailed information technology audit work completed by the GAO team. We believe that this work and your report will help us as we continue our efforts to improve the FDIC's information security program.

Overall the FDIC agrees with the results represented in the referenced draft reports and recognizes the need to broaden its test and evaluation program. In response to the recommendations for executive action, the FDIC will, by December 31, 2005:

- Complete corrective action for two of the remaining control weaknesses identified in the 2003 review;
- Correct the 20 information systems control weaknesses identified in this year's review; and
- Broaden the Corporation's computer security test and evaluation program to ensure that all key areas supporting FDIC's financial environment are routinely reviewed and tested.

Appendix I
Comments from the Federal Deposit
Insurance Corporation

Mr. Gregory C. Wilshusen

- 2 -

May 9, 2005

Corrective action for the remaining 2003 information systems control weakness, which we consider low risk, will be completed by February 28, 2006. Specific corrective action plans were provided separately.

I believe that significant progress has already been made in addressing the weaknesses identified in the draft reports. We understand that a sustained effort is needed through substantial resources and strong executive involvement to address the multitude of new vulnerabilities posed by the rapidly changing information technology industry. To that end, the FDIC remains committed to improving our corporate-wide security program. We look forward to continuing our productive dialogue with the GAO as we continue to enhance our security program.

If you have questions relating to the FDIC management response, please contact James Angel, Director, Office of Enterprise Risk Management, at 202-736-0138.

Sincerely,



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

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

GAO Contact and Staff Acknowledgments

GAO Contact

David W. Irvin, (214) 777-5716

Staff Acknowledgments

In addition to the individual named above, Edward Alexander Jr., Gerald Barnes, Jason Carroll, Lon Chin, Debra Conner, Anh Dang, Kristi Dorsey, Edward Glagola Jr., Nancy Glover, Rosanna Guerrero, David Hayes, Harold Lewis, Leena Mathew, Kevin Metcalfe, Duc Ngo, Eugene Stevens, Charles Vrabel, and Christopher Warweg 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