United States General Accounting Office

GAO

Report to the Board of Directors, Federal Deposit Insurance Corporation

May 2004

INFORMATION SECURITY

Information System Controls at the Federal Deposit Insurance Corporation

GAO-04-630

May 2004

INFORMATION SECURITY

Information System Controls at the Federal Deposit Insurance Corporation

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-630, a report to the Board of Directors, Federal Deposit Insurance Corporation

Why GAO Did This Study

Effective controls over information systems are essential to ensuring the protection of financial and personnel information and the security and reliability of bank examination data maintained by the Federal Deposit Insurance Corporation (FDIC). As part of our calendar year 2003 financial statement audits of three FDIC Funds, GAO assessed the effectiveness of the corporation's general controls on its information systems. Our assessment included follow up on the progress that FDIC has made in correcting or mitigating computer security weaknesses identified in our audits for calendar years 2001 and 2002.

What GAO Recommends

To establish an effective information system controls environment, GAO recommends that the FDIC Chairman instruct the chief information officer, who is the corporation's key official for computer security, to correct a number of information security weaknesses, including strengthening the testing and evaluation element of its computer security management program. 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-04-630.

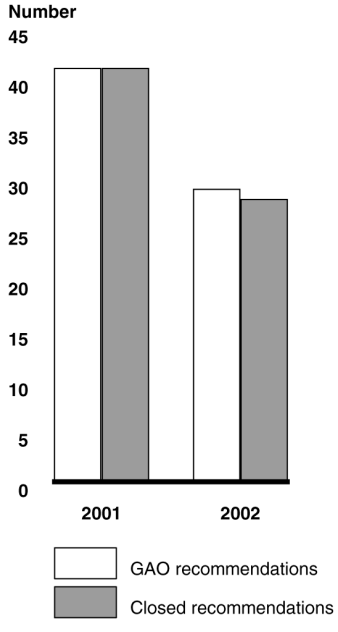
To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512- 3317 or daceyr@gao.gov.

What GAO Found

FDIC has made significant progress in correcting prior year information security weaknesses. The corporation addressed almost all the computer security weaknesses we previously identified in our audits for calendar years 2001 and 2002 (see figure). Nonetheless, testing in our calendar year 2003 audit identified additional computer control weaknesses in FDIC's information systems. These weaknesses place critical FDIC financial and sensitive examination information at risk of unauthorized disclosure, disruption of operations, or loss of assets.

A key reason for FDIC's continuing weaknesses in information system controls is that it has not yet fully established a comprehensive security management program to ensure that effective controls are established and maintained and that information security receives significant management attention. The corporation only recently established a program to test and evaluate its computer control environment, and this program does not yet include adequate provisions to ensure that (1) all key computer resources supporting FDIC's financial environment are routinely reviewed and tested, (2) weaknesses detected are analyzed for systemic solutions, (3) corrective actions are independently tested, and (4) newly identified weaknesses or emerging security threats are incorporated into the test and evaluation process.

FDIC Progress in Implementing GAO Recommendations



Source: GAO.

Contents

Abbreviations

CFO	Chief Financial Officer
CIO	Chief Information Officer
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Management Act
FSLIC	Federal Savings and Loan Insurance Corporation
ID	identification
IDS	intrusion-detection system

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

May 28, 2004

To the Board of Directors
Federal Deposit Insurance Corporation

As part of our calendar year 2003 financial statement audits of the Federal Deposit Insurance Corporation's (FDIC) Bank Insurance Fund, Savings Association Fund, and FSLIC (Federal Savings and Loan Insurance Corporation) Resolution Fund,[1] we assessed the effectiveness of the corporation's information system general controls.[2] Our assessment included follow-up on the progress that FDIC has made in correcting or mitigating computer security weaknesses in our audits for calendar years 2001[3] and 2002.[4] 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. Such controls also affect the security and reliability of nonfinancial information maintained by FDIC such as personnel and bank examination information.

This report summarizes weaknesses in information system controls over FDIC's computer systems. Because of the significance of these weaknesses, we reported information system controls as a reportable condition[5] in FDIC's financial statements audit report for calendar year

[1]U.S. General Accounting Office, *Financial Audit: Federal Deposit Insurance Corporation Fund's 2003 and 2002 Financial Statements*, GAO-04-429 (Washington, D.C.: Feb. 13, 2004).

[2]Information system general controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. These controls include security management, operating procedures, software security features, and physical 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 back-up and recovery plans are adequate to ensure the continuity of essential operations.

[3]U.S. General Accounting Office, *FDIC Information Security: Improvements Made but Weaknesses Remain*, GAO-02-689 (Washington, D.C.: July 15, 2002).

[4]U.S. General Accounting Office, *FDIC Information Security: Progress Made but Existing Weaknesses Place Data at Risk*, GAO-03-630 (Washington, D.C.: June 18, 2003).

[5]Reportable 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.

2003.[6] We are also issuing a report designated for "Limited Official Use Only," which describes in more detail the computer security weaknesses identified and offers specific recommendations for correcting them.

We performed our review at FDIC headquarters in Washington, D.C., and at its computer facility in Arlington, Virginia, from September 2003 through January 2004. Our review was performed in accordance with U.S. generally accepted government auditing standards.

Results in Brief

Although FDIC has made significant progress in correcting prior year information security weaknesses, systems still remain vulnerable due to weaknesses in information system general controls. FDIC addressed almost all of the computer security weaknesses we previously identified in our audits for calendar years 2001 and 2002 and has taken other steps to improve security since last year's audit. Nonetheless, testing in our calendar year 2003 audit identified additional computer control weaknesses in the corporation's information systems. Specifically, FDIC had not adequately limited the access granted to all authorized users or completely secured access to its network. The risk created by these access weaknesses was heightened because FDIC had not completed a program to fully monitor access activity to identify and investigate unusual or suspicious access patterns that could indicate unauthorized access. As a result, critical financial and sensitive personnel and bank examination information was at risk of unauthorized disclosure, disruption of operations, or loss of assets.

A key reason for FDIC's continuing weaknesses in information system controls is that it had not yet fully established a comprehensive security management program to ensure that effective controls are established. An effective program includes a central security function that assesses risk, establishes appropriate policies and related controls, raises awareness of prevailing risks, and routinely tests and evaluates the effectiveness of established controls. FDIC made substantial progress during the past year in establishing key elements of a security program, including strengthening its security management structure, updating security policies and procedures, enhancing security awareness training, and implementing a risk assessment program. However, it only recently established a program

[6]GAO-04-429.

to test and evaluate its computer control environment, and this program does not yet address all key areas. Specifically, the program does not include adequate provisions to ensure that (1) all key computer resources supporting FDIC's financial environment are routinely reviewed and tested, (2) weaknesses detected are analyzed for systemic solutions, (3) corrective actions are independently tested, and (4) newly identified weaknesses or emerging security threats are incorporated into the test and evaluation process.

We are making a recommendation to fully establish a comprehensive computer security management program to strengthen the testing and evaluation element of FDIC's program. In a separate report designated "Limited Official Use Only," we are making recommendations to correct the specific weaknesses identified during our review.

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 1933 to restore and maintain public confidence in the nation's banking system. The Financial Institutional Reform, Recovery, and Enforcement Act of 1989 sought to reform, recapitalize, and consolidate the federal deposit insurance system. 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, respectively, from loss due to institutional failures. The act also 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 $3.3 trillion for about 9,200 institutions. Together, the three funds have about $49.5 billion in assets. FDIC had a budget of about $1.1 billion for calendar year 2003 to support its activities in managing the three funds. For that year, it processed more than 2.6 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 6,300 individuals were authorized to use FDIC's systems. FDIC's chief information officer (CIO) is the corporation's key official for computer security. The CIO is responsible for establishing, implementing, and overseeing a corporatewide information security program.

Information security is a critical consideration for any organization that depends on information systems and networks to carry out its mission or business. Without proper safeguards, there is enormous 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 actions to address the risks associated with persistent information security weaknesses. In December 2002, the Federal Information Security Management Act (FISMA), 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 have issued security guidance to agencies.

[7]See, for example, U.S. General Accounting Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructure*, GAO-03-121 (Washington, D.C.: January 2003).

[8]Title III, Federal Information Security Management Act of 2002, E-Government Act of 2002, P.L. 107-347 (Dec. 17, 2002).

Objective, Scope, and Methodology

The objective of our review was to assess the effectiveness of FDIC's information system general controls, including the progress the corporation had made in correcting or mitigating weaknesses reported in our financial statement audits for calendar years 2001[9] and 2002.[10] Our evaluation was based on (1) our *Federal Information System Controls Audit Manual*,[11] which contains guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data, and (2) our May 1998 report on security management best practices[12] at leading organizations, which identifies key elements of an effective information security program.

Specifically, we evaluated information system controls intended to

- protect data and software from unauthorized access;
- prevent the introduction of unauthorized changes to application and system software;
- provide segregation of duties involving application programming, system programming, computer operations, information security, and quality assurance;
- ensure recovery of computer process operations 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, and conducted tests and observations of controls in operation. In addition, we reviewed FDIC's corrective actions

[9]U.S. General Accounting Office, *Financial Audit: Federal Deposit Insurance Corporation Fund's 2002 and 2001 Financial Statements*, GAO-03-543 (Washington, D.C.: Mar. 28, 2003).

[10]GAO-04-429.

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

[12]U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

taken to address vulnerabilities identified in our audits for calendar years 2001 and 2002.

Improvements Were Made in Correcting Prior Year Weaknesses, but Systems Remain Vulnerable

In 2001[13] and again in 2002,[14] we reported computer security weaknesses at FDIC, including specific weaknesses related to mainframe and network security, physical access, application change control, and service continuity. These weaknesses placed critical corporation operations at risk of misuse and disruption. Although FDIC has made significant progress in correcting these weaknesses and has taken other steps to improve security, our testing in our calendar year 2003 audit identified additional control weaknesses. Specifically, FDIC had not adequately limited the access granted to all authorized users or completely secured access to its network. Further, FDIC had not yet completed a program to fully monitor user activities for unusual or suspicious patterns that could indicate unauthorized access. As a result, critical FDIC financial and sensitive personnel and bank examination information was at risk of unauthorized disclosure, disruption of operations, or loss of assets—possibly without detection. A key reason for FDIC's weaknesses is that it had not yet fully implemented a comprehensive security management program.

FDIC Has Taken Action to Correct Prior Year Weaknesses and Improve Security

FDIC has made significant progress in correcting previously identified information security weaknesses. FDIC took action to address current and prior year weaknesses, including completing action on (1) the 22[15] weaknesses that remained open from our 2001 audit[16] and (2) 28 of the 29 weaknesses from our 2002 audit.[17] Specifically, FDIC

[13]GAO-02-689.

[14]GAO-03-630.

[15]GAO identified 41 weaknesses in the 2001 review; FDIC addressed 19 of those weaknesses before our next review.

[16]GAO-02-689.

[17]GAO-03-630.

- reduced user access to sensitive program libraries and critical financial and sensitive data,
- strengthened security over certain network platforms,
- expanded its application software change control procedures to include all software changes,
- developed and implemented disaster recovery plans for all its major systems and incorporated unannounced testing procedures into its service continuity process, and
- enhanced system software change control processes.

In addition to responding to previously identified weaknesses, FDIC established several other computer controls to enhance its information security. For example, it established procedures for securing new remote access and private network services. In addition, it strengthened security procedures over its system that handles large files submitted to FDIC by banking institutions. Further, FDIC initiated reviews of its network infrastructure as a precursor to establishing an ongoing program of tests and evaluations of its computer environment.

Access Authority Was Not Appropriately Limited for All Users

A basic management control objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modification, disclosure, or deletion. Organizations can protect this critical information by granting employees the authority to read or modify only those programs and data that they need to perform their duties and by periodically reviewing access granted to ensure it is appropriate. Effective access controls should be designed to restrict access to computer programs and data and prevent and detect unauthorized access. These controls include assigning user access rights and permissions and ensuring that access remains appropriate on the basis of job responsibilities.

Although FDIC restricted access to certain data and programs on its systems, we identified instances in which access to sensitive data and programs had not been sufficiently restricted. For example:

- Many users had unnecessary access to production systems that includes financial and bank information. These users were inadvertently granted access to the systems that could allow these users to gain access to critical financial management information. This vulnerability was further heightened because an undetermined number of the users were system developers. These developers have detailed knowledge of the systems' processing functions; knowledge that could allow them to improperly add, alter, or delete critical financial and sensitive information or programs—possibly without detection.

- A large number of users had access that allowed them to read a powerful user identification (ID) and password used to transfer data among FDIC production computer systems. With this ID and password, the users could gain unauthorized access to financial and sensitive corporation information—possibly without detection.

- FDIC did not adequately restrict users from viewing sensitive information. For example, all network users had unrestricted read access to sensitive bank information. Failure to adequately control access to this type of information could result in users gaining unauthorized access to privileged information.

Although FDIC has initiated actions to correct these weaknesses, the access vulnerabilities continue because the corporation has not yet fully established a process for reviewing the appropriateness of individual access privileges. Specifically, FDIC's process did not include a comprehensive method for identifying and reviewing all access rights granted to any one user. Such reviews would have allowed FDIC to identify and correct inappropriate access.

In response, FDIC said that it has since taken steps to restrict access to critical financial data and programs and related sensitive information. Further, the corporation stated that it enhanced its process for identifying and reviewing user access granted and was establishing a policy that will require quarterly reviews of users with broad access privileges.

Network Security Improved, but Some Weaknesses Continue

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 and transmitted along networks, effectively securing networks is essential for protecting computing resources and data from unauthorized access, manipulation, and use.

Organizations can secure their networks, in part, by limiting the services that are available on the network and by installing and configuring network devices that permit authorized network service requests and deny unauthorized requests. Network devices include (1) firewalls designed to prevent unauthorized access into the network, (2) routers that filter and forward data along the network, (3) switches that filter and forward information among parts of a network, and (4) servers that host applications and data. Insecurely configured network services and devices can make a system vulnerable to internal or external threats, such as hackers, cyberterrorist groups, and denial-of-service attacks. Since networks provide the entry point for access to electronic information assets, failure to secure them increases the risk of the unauthorized use of sensitive data and systems.

FDIC continued to take steps to secure its network through enhancements to its firewall and specific network platforms. Further, it established processes to strengthen the security of its local area network and password management. In addition, FDIC initiated a testing cycle to review the effectiveness of information system controls for specific network resources. Nonetheless, we identified weaknesses in the way that FDIC managed network services, controlled network connectivity, and maintained network software, as the following examples demonstrate.

- A network service was not configured to restrict access to sensitive network resources. As a result, anyone—including contractors—with access to the FDIC network could obtain copies or modify configuration files containing control information such as access control lists. With the ability to read, copy, or modify these files, an intruder could disable or disrupt network operations by taking control of sensitive and critical network resources.

- Access connectivity to critical network resources was not adequately restricted. With connectivity to these key resources, an unauthorized user could attempt to exploit network vulnerabilities and gain control of key segments of the network.

- Certain network connections to off-site locations were not adequately controlled. These connections are essential to securing operations of the network they serve. Ineffectively secured network connections could expose the internal network to unauthorized access and make it easier for this access to go undetected.

Further, FDIC did not consistently secure its network against known software vulnerabilities or minimize the operational impact of potential failure in a critical network device. Failure to address known vulnerabilities increases the risk of system compromise, such as unauthorized access to and manipulation of sensitive system data, disruption of services, and denial of service.

In responding to our findings, FDIC's CIO said that the corporation had taken steps to improve network security. Specifically, he said that FDIC had reconfigured network resources to restrict access, made software modifications to secure against known vulnerabilities, and established a process for assessing contractor connectivity requirements.

Program to Fully Monitor Access Was Not Complete

The risks created by these access and network security weaknesses were heightened because FDIC had not yet completed a program to fully monitor user activities. Such a program to monitor access would include routinely reviewing user access activity and investigating failed attempts to access sensitive data and resources, as well as unusual and suspicious patterns of successful access to sensitive data and resources.

To effectively monitor user access, it is critical that logs of user activity be maintained for all critical processing activities. This includes collecting and monitoring activities on all critical systems, including mainframes, network servers, and routers. A comprehensive monitoring program should include an intrusion-detection system (IDS) that monitors all key network resources and automatically logs unusual activity, provides necessary alerts, and terminates access. Further, to safeguard IDS operations and the access information it collects, the duties and responsibilities of staff assigned to the monitoring program should be adequately segregated.

Although FDIC has made progress in developing systems to identify unauthorized or suspicious access activities for both its mainframe and network systems, its program as implemented does not fully monitor for such activities. As a result, there are weaknesses in FDIC's monitoring program that could result in significant breaches to its computer security environment. For example, the network IDS did not monitor all network traffic originating from certain locations. Further, certain network resources were not configured to monitor network traffic, which lessens the corporation's ability to identify anomalies. In addition, responsibilities for operating the IDS were not appropriately segregated. For example, the corporation assigned the responsibilities for design, implementation, and

maintenance to one individual. By assigning these functions to one person, it did not adequately ensure a system of checks and balances. Thus, FDIC is at risk that its program designed to monitor access activities for unusual or suspicious activities could be altered to allow unauthorized system actions that could go undetected.

In response to our findings, FDIC's CIO said that the corporation had developed and begun implementation of a monitoring strategy for information technology security. This includes monitoring, event correlations, and incident identification and response. Further, the corporation plans to hire additional staff to allow it to segregate responsibilities for operating the IDS.

Substantial Progress Was Made in Implementing a Computer Security Program, but a Key Element Was Incomplete

A key reason for FDIC's continuing weaknesses in information system controls is that it has not yet fully established a comprehensive security management program to ensure that effective controls are established and maintained and that information security receives significant management attention. Our May 1998 study[18] of security management best practices determined that a comprehensive information security management program is essential to ensuring that information system controls work effectively on a continuing basis. The recently enacted FISMA, consistent with our study, describes certain key elements of a comprehensive information security management program. These elements include

- a central 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 security environment;
- 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, about information security risks

[18]GAO/AIMD-98-68.

and the responsibilities of these individuals in complying with agency policies and procedures;

- 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; and

- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices—to be performed with a frequency depending on risk, but no less than annually—that include testing of management, operational, and technical controls of major information systems.

During the past year, FDIC made substantial progress in establishing a comprehensive computer security management program. As discussed below, FDIC has (1) strengthened its central security management structure, (2) updated its security policies and procedures, (3) enhanced its security awareness training, and (4) developed a risk assessment program.

- *Central security management structure.* FDIC strengthened accountability and authority for its previously established central security management function by appointing a permanent CIO who reports directly to the chairman. Further, FDIC realigned its security management function so that it reports directly to the CIO. Also, FDIC provided additional staff management resources to oversee its certification and accreditation process, system test and evaluation program, computer security incident response team activities, and firewall administration. Additionally, other staff resources were added to maintain and enhance security policies and procedures and provide oversight to the corporation's newly established risk assessment and test and evaluation programs.

- *Security policies and procedures.* FDIC enhanced its overall security policies covering network security, computer center access, mainframe controls, and security management. For example, it developed new policies covering controls for the use of wireless networks and requirements for patch management. In addition, it developed network security procedures to ensure compliance with policy on the use of default vendor accounts, restrictions on network services, and adherence to network password standards. Further, FDIC strengthened its policies on requesting and granting access to its computer center and

provided updated requirements to address weaknesses in its configuration management procedures for financial system changes. Also, the corporation issued new policies on performing risk assessments of its security program and information systems.

- *Security awareness training.* FDIC enhanced its current security awareness program for employees and contractors. Specifically, it updated the program to reflect FISMA security requirements, new policies and procedures developed to mitigate newly identified security risks, and discussions of internal threats. The corporation also developed specialized security awareness training to address the needs of selected technical staff and enhanced its reporting process to ensure that all security awareness training is reported.

- *Risk assessments.* Recently, FDIC developed a framework for assessing and managing risk on a continuing basis. This framework specifies (1) how the assessments should be initiated and conducted, (2) who should participate in the assessment, (3) how disagreements should be resolved, (4) what approvals are needed, and (5) how these assessments should be documented and maintained. At the completion of our audit, the corporation had performed risk assessments on all of its major systems.

Although FDIC has made substantial progress in each of the elements discussed above, it only recently established a program to test and evaluate its computer control environment, but this program was incomplete. Test and evaluation is a key element of an information security program that includes ongoing reviews, tests, and evaluations of information security to ensure that systems are in compliance with policies and procedures and to identify and correct weaknesses that may occur. FDIC began implementing this program during 2003. In October 2003, the corporation used a contractor to (1) develop a self-assessment process that includes annual general and application control reviews and (2) begin to perform ongoing quarterly tests of its systems. Still, FDIC's test and evaluation program does not address all key areas. Specifically, the program does not include the following provisions.

- *All key computer resources supporting FDIC's financial systems are routinely reviewed and tested, as appropriate.* FISMA requires agencies to develop, document, and implement an agencywide information security program that includes routine security reviews of key computer resources supporting critical information systems, such

as those supporting the corporation's financial systems. These reviews should include those managed by other agencies or contractors. Although it initiated a program of tests and evaluations, this program did not yet address all key computer resources. For example, FDIC relies extensively on contractors to support its financial systems, and accordingly, provides them with connections and access to its internal network. Yet, during the past 2 years, the corporation has performed only limited security reviews of these contractor connections—a key computer resource. Further, FDIC did not schedule a review of these contractor connections in conjunction with its newly established self-assessment process. Without routine tests and evaluations of all key computer resources, including contractor connections, the corporation's financial or sensitive bank information is at risk of unauthorized disclosure, disruption of operations, or loss of assets.

- *Information security weaknesses detected are analyzed for systemic solutions.* To ensure that actions taken to correct identified security weaknesses are effective, security management best practices prescribe that procedures should include an assessment of systemic causes of related security weaknesses. Although FDIC has been very proactive in addressing the individual information security weaknesses identified, it currently lacks an ongoing process to collectively analyze related weaknesses for systemic problems that could adversely affect critical financial and bank information systems. A comprehensive assessment of related weaknesses, such as those related to user access privileges, which is a recurring security weakness we have reported to FDIC, could assist in identifying systemic causes of security weaknesses and result in remediation efforts that could be more effective in addressing security vulnerabilities. Further, such an assessment provides an organization with a process of identifying emerging problems, assessing the effectiveness of current policies and awareness efforts, and determining the need for stepped-up education or new controls to address problem areas.

- *Corrective actions are independently tested.* FISMA requires that agencies establish a process to document and track remedial actions taken to address security deficiencies in agency operations. This process includes requirements for independent testing to ensure that prescribed remediation actions are effective. Although FDIC has established a system for documenting and tracking corrective actions, it has not developed a specific process for independently testing or reviewing the appropriateness of the corrective actions taken.

- *Newly identified weaknesses or emerging security threats are incorporated into the test and evaluation process.* To ensure an effective test and evaluation program, security management best practices prescribe that the scope of information system control tests include an evaluation of recently identified weaknesses and an assessment of emerging security threats to the computer control environment. FDIC's self-assessment process includes provisions for updating its annual review of information system controls to evaluate control weaknesses that were identified in prior audits. However, the process does not specifically include provisions for weaknesses reported in other audits or those identified internally in connection with operational issues. Further, there are no procedures to ensure that emerging security threats are considered for inclusion in the self-assessment reviews. For example, in our current review at FDIC, we identified network security weaknesses that are linked to specific new security threats that had not been addressed by FDIC. To perform a comprehensive review of information system controls, it is critical that all previously identified weaknesses and emerging security threats be considered as part of the test and evaluation process to ensure that these weaknesses have been corrected.

Incorporating these key areas into its test and evaluation program should allow FDIC to better identify and correct security problems, such as those identified in our 2003 audit.

Conclusions

FDIC has made significant progress in correcting the computer security weaknesses we previously identified and has taken other steps to improve security. However, we identified additional computer control weaknesses that place critical FDIC financial and sensitive personnel and bank examination information at risk of unauthorized disclosure, disruption of operations, or loss of assets. Specifically, FDIC had not adequately limited the access granted to all authorized users or completely secured access to its network. The risks created by these access weaknesses are heightened because FDIC has not yet completed a program to fully monitor access activity to identify and investigate unusual or suspicious access patterns that could indicate unauthorized access. Implementation of FDIC's plan to correct these weaknesses is essential to establishing an effective information system control environment.

A key reason for FDIC's continuing weaknesses in information system controls is that it has not yet fully established a comprehensive security

management program to ensure that effective controls are established and maintained and that information security receives significant management attention. Although FDIC has made substantial progress during the past year toward establishing key elements of this program—including strengthening its security management structure, updating security policies and procedures, enhancing security awareness, and implementing a risk-assessment program—it only recently established a program to test and evaluate its computer control environment, and this program does not yet address all key areas. Specifically, the test and evaluation program does not include adequate provisions to ensure that (1) all key computer resources supporting FDIC's financial environment are routinely reviewed and tested, (2) weaknesses detected are analyzed for systemic solutions, (3) corrective actions are independently tested, and (4) newly identified weaknesses or emerging security threats are incorporated into the test and evaluation process. Until FDIC takes steps to correct or mitigate its information system control weaknesses and fully implements a computer security management program, FDIC will have limited assurance that its financial and sensitive information is adequately protected.

Recommendations for Executive Action

To fully establish a comprehensive computer security management program, we recommend that the FDIC chairman instruct the CIO, as the corporation's key official for computer security, to strengthen the testing and evaluation element of this program by taking the following actions:

- all key computer resources supporting FDIC's financial environment should be routinely reviewed and tested,
- weaknesses detected should be analyzed for systemic solutions,
- corrective actions should be independently tested, and
- newly identified weaknesses or emerging security threats should be incorporated into the test and evaluation process.

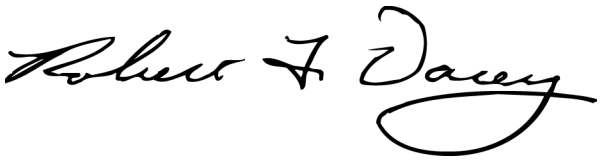
We are also making recommendations in a separate report designed for "Limited Official Use Only." These recommendations address actions needed to correct the specific information security weaknesses related to user access, network security, and monitoring access activities.

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 the information system control weaknesses identified and strengthen the testing and evaluation element of its computer management program by December 31, 2004. 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 will also make copies available to other parties 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) 512-3317 or David W. Irvin, Assistant Director, at (214) 777-5716. We can also be reached by e-mail at daceyr@gao.gov and irvind@gao.gov, respectively. Key contributors to this report are listed in appendix II.



Robert F. Dacey
Director, Information Security Issues

Comments from the Federal Deposit Insurance Corporation

FDIC
Federal Deposit Insurance Corporation
550 17th Street, NW, Washington, DC 20429
Deputy to the Chairman and Chief Financial Officer

May 4, 2004

Mr. Joel C. Willemssen, Managing Director
Information Technology Issues
U.S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Willemssen:

Thank you for the opportunity to respond to the draft reports entitled, Information Security: Information System Controls at the Federal Deposit Insurance Corporation, dated April 26, 2004. We appreciate the generally positive tone of these reports, particularly in the General Accounting 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 FDIC's completion of 69 of 70 recommended security improvements from the 2001 and 2002 GAO audit reports.

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 fully developed and implemented a comprehensive corporate program to manage security, particularly a program to test and evaluate its computer control environment. 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 overall information security program.

Overall the FDIC agrees with the results represented in the referenced draft reports and recognizes the need to further enhance its existing programs. We believe that it is important to note that our activities have essentially moved from program development to enhancement or fine tuning of individual program activities. In response to the recommendations for executive action, the FDIC will, by December 31, 2004:

- Complete corrective action for the one remaining control weakness identified in the 2002 review;
- Correct the 22 information systems control weaknesses identified in this year's review; and
- Continue to enhance the Corporation's computer security testing and evaluation program including ensuring: (1) all key computer resources supporting FDIC's financial environment are routinely reviewed and tested, 2) weaknesses detected are

analyzed for systematic solutions, 3) corrective actions are independently tested, and 4) newly identified weaknesses or emerging security threats are incorporated into the test and evaluation process.

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 every aspect of 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 Michael MacDermott, Acting Director, Office of Enterprise Risk Management, at 202-736-0075.

Sincerely,

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

cc: John Bovenzi
John Brennan
Michael Bartell
Michael MacDermott
Audit Committee

GAO Contact and Staff Acknowledgments

GAO Contact

David W. Irvin, (214) 777-5716

Staff Acknowledgments

In addition to the person named above, Edward Alexander, Jr., Gerald Barnes, Nicole Carpenter, Lon Chin, Debra Conner, David Hayes, Jeffrey Knott, Leena Mathew, Duc Ngo, Rosanna Villa, Charles Vrabel, and Chris Warweg made key contributions to this report.

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

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. General Accounting 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

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00