United States General Accounting Office

GAO

Report to the Board of Directors, Federal Deposit Insurance Corporation

June 2003

FDIC INFORMATION SECURITY

Progress Made but Existing Weaknesses Place Data at Risk

GAO-03-630

June 2003

FDIC INFORMATION SECURITY

Progress Made but Existing Weaknesses Place Data at Risk

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-630, 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 GAO's 2002 financial statement audits of the three FDIC funds, we assessed (1) the corporation's progress in addressing computer security weaknesses found in GAO's 2001 audit, and (2) the effectiveness of FDIC's controls.

What GAO Recommends

In order to establish an effective information system control environment, in addition to fully addressing the recommendations stemming from the 2001 review, GAO recommends that the Chairman instruct the acting chief information officer to ensure that actions are completed to correct the weaknesses identified during GAO's 2002 review. In commenting on a draft of this report FDIC agreed with our recommendations. FDIC plans to address the identified weaknesses and stated that significant progress has already been made.

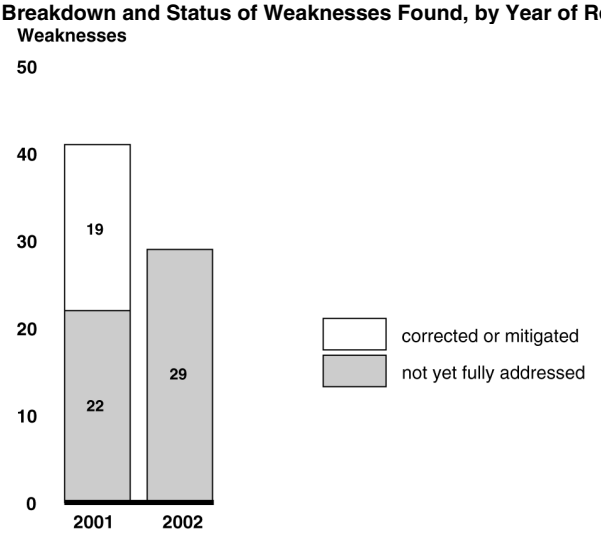
www.gao.gov/cgi-bin/getrpt?GAO-03-630.

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

What GAO Found

FDIC has made progress in correcting information system controls since GAO's 2001 review. Of the 41 weaknesses identified that year, FDIC has corrected or has specific action plans to correct all of them (see figure). GAO's 2002 audit nonetheless identified 29 new computer security weaknesses. These weaknesses reduce the effectiveness of FDIC's controls to safeguard critical financial and other sensitive information.

Breakdown and Status of Weaknesses Found, by Year of Review



Source: GAO.

Based on our review, mainframe access was not sufficiently restricted, network security was inadequate, and a program to fully monitor access activities was not implemented. Additionally, weaknesses in areas including physical security, application software, and service continuity further increased the risk to FDIC's computing environment.

The primary reason for these continuing weaknesses is that FDIC has not yet completed development and implementation of a comprehensive program to manage computer security across the organization. FDIC has, among other things, established a security management structure, but still has not fully implemented a process for assessing and managing risk on a continuing basis or an ongoing program of testing and evaluating controls. The corporation's acting chief information officer has agreed to complete actions intended to address GAO's outstanding recommendations by December 31 of this year.

Contents

GAO
Accountability * Integrity * Reliability

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

June 18, 2003

To the Board of Directors
Federal Deposit Insurance Corporation

As part of our calendar year 2002 financial statement audits of the Federal Deposit Insurance Corporation's (FDIC) Bank Insurance Fund, Savings Association Insurance Fund, and FSLIC (Federal Savings and Loan Insurance Corporation) Resolution Fund,[1] we assessed (1) the progress FDIC has made in correcting or mitigating computer security weaknesses reported in our calendar year 2001 audit,[2] and (2) the effectiveness of the corporation's information system general controls.[3] 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 such as personnel and bank examination information maintained by FDIC.

This report summarizes weaknesses in information systems controls over FDIC's computer systems. Because of the significance of these weaknesses, we reported information system controls as a reportable condition[4] in FDIC's financial statements audit report for calendar year 2002.[5] We are also issuing a report designated for "Limited Official Use

[1]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).

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

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

[4]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.

[5]GAO-03-543.

Only," which describes in more detail the computer security weaknesses identified and offers specific recommendations for correcting them.

Results in Brief

FDIC has made progress in correcting information system control weaknesses and implementing controls since our calendar year 2001 audit. Of the 41 weaknesses identified, FDIC has corrected 19 and is taking action to resolve the 22 that remain.

However, testing this year identified additional weaknesses in information system controls. Such weaknesses reduce the effectiveness of FDIC's controls to safeguard electronic access to critical financial and other sensitive information. When combined with unaddressed weaknesses for the previous year, the risk of unauthorized disclosure of critical financial and other sensitive information, disruption of critical operations, and loss of assets is increased. Specifically, FDIC weaknesses include not sufficiently restricting mainframe access, adequately securing its network, or implementing a program to fully monitor access activity. In addition, weaknesses in other information system controls, including physical security, application software, and service continuity, further increase the risk to FDIC's information systems.

The key reason for FDIC's continuing weaknesses in information system controls is that it has not yet fully developed and implemented a comprehensive corporate program to manage computer security. An effective program would include assessing risks, establishing appropriate policies and related controls, raising awareness of prevailing risks and mitigating controls, and evaluating the effectiveness of established controls. FDIC has established a security management structure, implemented security policies and procedures, and enhanced security awareness training, but it has not fully implemented a process for assessing and managing risk on a continuing basis, or a comprehensive, ongoing program of testing and evaluation to ensure that policies and controls are appropriate and effective.

To establish an effective information system control environment, in addition to fully addressing recommendations stemming from the 2001 review, we are making recommendations to ensure that actions are completed to correct those weaknesses identified in this year's audit. In response, the acting chief information officer (CIO) stated that he has agreed to take action intended to correct the weaknesses by December 31, 2003.

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 Institutions Reform, Recovery, and Enforcement Act of 1989 sought to reform, recapitalize, and consolidate the federal deposit insurance system. It created the Bank Insurance Fund and the Savings Association Insurance Fund, 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 9,400 institutions. Together the three funds have about $49.5 billion in assets. FDIC had a budget of about $1.2 billion for calendar year 2002 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 7,000 individuals were authorized to use FDIC's systems. FDIC's acting CIO is the corporation's key official for computer security.

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 our calendar year 2001 financial statement audit[6] and (2) the effectiveness of information system general controls. These information system controls also affect the security and reliability of other sensitive data, including personnel, legal, and bank examination information maintained on the same computer systems as the corporation's financial information. Our evaluation was based on (1) our *Federal Information System Controls Audit Manual*, 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[7] 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 processing operations in case of disaster or other unexpected interruption; and
- ensure an adequate information security management 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 corrective actions taken by FDIC to address vulnerabilities identified in our calendar year 2001 audit.

[6]GAO-02-689.

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

We performed our review at FDIC's headquarters in Washington, D.C.; its computer facility in Arlington, Virginia; and FDIC's Dallas regional office, from October 2002 through March 2003. Our review was performed in accordance with U.S. generally accepted government auditing standards.

FDIC Has Made Progress in Correcting Weaknesses and Implementing Controls

FDIC has made progress in correcting previously identified computer security weaknesses. Of the 41 weaknesses identified in our calendar year 2001 audit,[8] FDIC has corrected 19 and is taking action intended to resolve the 22 that remain. FDIC has addressed key access control, application software, system software, and service continuity weaknesses previously identified. Specifically, FDIC

- limited access to certain critical programs, software, and data;
- reduced the number of users with physical access to computer facilities;
- enhanced its review procedures of system software changes;
- strengthened its procedures for reviewing changes to application software;
- expanded tests of its disaster recovery plan; and
- defined the roles and responsibilities of its information security officers.

In addition to responding to previously identified weaknesses, FDIC established several other computer controls to enhance its information security. For example, it enhanced procedures to periodically review user access privileges to computer programs and data to ensure that access is granted only to those who need it to perform their jobs. Likewise, FDIC strengthened its physical security controls by establishing criteria for granting access to computer center operations, and developed procedures for periodically reviewing access to ensure that it remained appropriate.

Further, FDIC enhanced its system software change control process by developing procedures requiring technical reviews of all system software modifications prior to their implementation. In addition, it established a

[8] GAO-02-689.

process to periodically review application software to ensure that only authorized computer program changes were being made. FDIC also improved its disaster recovery capabilities by establishing an alternate backup site to support its computer network and related system platforms, and by conducting periodic unannounced walk-through tests of its disaster recovery plan.

The following sections summarize the results of our review. Our "Limited Official Use Only" report details specific weaknesses in information systems controls that we identified, provides our recommendations for correcting each weakness, and indicates FDIC's planned actions or those already taken for each weakness. An evaluation of the adequacy of this action plan will be part of our future work at FDIC.

Weaknesses Continue to Place Financial and Sensitive Data at Risk

Although FDIC established many policies, procedures, and controls to protect its computing resources, the corporation did not always effectively implement them to ensure the confidentiality, integrity, and availability of financial and sensitive data processed by its computers and networks. In addition to the previously reported weaknesses that remain not fully addressed, 29 new information security weaknesses were identified during this review.

The weaknesses identified included instances in which FDIC did not adequately restrict mainframe access, secure its network, or establish a complete program to monitor access activities. In addition, new weaknesses in other information system controls, including physical security, application software, and service continuity, further increase the risk to FDIC's information systems. Collectively they place the corporation's systems at risk of unauthorized access, which could lead to unauthorized disclosure, disruption of critical operations, and loss of assets.

Mainframe Access Was Not Adequately Restricted

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 that it is appropriate. Effective mainframe access controls should be designed to

restrict access to computer programs and data, and prevent and detect unauthorized access. These controls include access rights and permissions, system software controls, and software library management.

While FDIC restricted access to many users who previously had broad access to critical programs, software, and data, instances remained in which the access granted specific users was still not appropriate. A key weakness in FDIC's controls was that it did not adequately limit user access, as described below.

- Nineteen users had access to production control software that would allow them to modify software outside the formal configuration control process. This risk was further heightened because FDIC was not maintaining audit logs of software changes. Without such logs, unauthorized software changes could be made to critical financial and sensitive systems, possibly without detection. This software was especially vulnerable because it could allow an unauthorized user to bypass security controls. Further, an excessive number of users had access to 14 of 19 production job control systems we reviewed, allowing them to obtain exact details of production programs and data, which could then be used to gather information to circumvent controls.

- An excessive number of users had access that allowed them to read user identifications (IDs) and passwords used to transfer data among FDIC production computer systems. With these IDs and passwords, 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, about 70 users had unrestricted read access to all information that the corporation printed from its mainframe computer. This included information on bank examinations, payroll and personnel data, legal reports, vendor payments, and security monitoring information.

One reason for FDIC's user access vulnerabilities was that the corporation, while making progress, still had not 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 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 sensitive resources. Further, the corporation stated that it has improved its audit logging of user access activities, enhanced its process for identifying and reviewing access granted, and further reduced access to the minimum necessary for users to perform their job functions.

Network Security Improved, but Some Weaknesses Continue

Network security controls are key to ensuring that only authorized individuals gain access to sensitive and critical agency data. Effective network security controls should be established to authenticate local and remote users. These controls include a variety of tools such as user passwords, intended to authenticate authorized users who access the network from local and remote locations. In addition, network controls provide safeguards to ensure that system software is adequately configured to prevent users from bypassing network access controls or causing network failures.

Since our last audit, FDIC took major steps to secure its network through enhancements to its firewall and establishment of procedures to review contractor network connections; further, it recently implemented actions to review the effectiveness of network security controls. Nonetheless, weaknesses in the way the corporation configured its network servers, managed certain user IDs and passwords, and provided network services have not yet been corrected.

- One system was using a default vendor account with broad access that would allow the user to read, copy, modify, or delete sensitive network configuration files. Information on default vendor accounts is available in vendor-supplied manuals, which are readily available to hackers. With this ability, a malicious user or intruder could seriously disable or disrupt network operations by taking control of key segments of the network or by gaining unauthorized access to critical applications and data.

- 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 and user passwords. 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.

- A key network server was not adequately configured to restrict access. As a result, anyone—again, including contractors—with connectivity to the FDIC network could copy or modify files containing sensitive network information. With this level of access, an unauthorized user could control key segments of the network.

Further, FDIC did not adequately secure its network against known vulnerabilities or minimize the operational impact of a 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 response to our findings, FDIC's acting CIO said that the corporation had taken steps to improve network security. Specifically, he said that FDIC had removed the vendor default account, reconfigured network resources to restrict access, and installed software patches to secure against known vulnerabilities.

Program to Fully Monitor Access Activities Not Complete

A program to monitor access activities is essential to ensuring that unauthorized attempts to access critical programs and data are detected and investigated. Such a program 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 to automatically log unusual activity, provide necessary alerts, and terminate access.

While FDIC has made progress in developing systems to identify unauthorized or suspicious access activities for both its mainframe and network systems, it still has not completed a program to fully monitor such activities. As a result, reports designed to provide security staff with information on network access activities, including information on unusual or suspicious access, were not available due to technical problems in producing them. Consequently, security staff and administrators did not

have the information they needed to effectively monitor the network for unauthorized or inappropriate access.

Further, FDIC was not monitoring the access of certain employees and contractors with access that allowed them to modify specific sensitive system software libraries that can perform functions that circumvent all security controls. While these users were granted these access privileges, FDIC did not maintain audit logs of access to ensure that only authorized modifications were made to these libraries. As a result, these users could make unauthorized modifications to financial data, programs, or system files, possibly without detection.

According to the acting CIO, the corporation has taken action to improve its program to monitor access activities. This includes developing and implementing new reports for monitoring network access and initiating action to fully implement its intrusion-detection system.

Other Information System Controls Were Also Ineffective

In addition to information system access controls, other important controls necessary to ensure the confidentiality, integrity, and availability of an organization's system and data were ineffective at FDIC. These controls include policies, procedures, and techniques that physically secure data-processing facilities and resources, prevent unauthorized changes to application software, and effectively ensure the continuation of computer processing service if an unexpected interruption occurs. Although FDIC has implemented numerous information system controls, remaining weaknesses in these areas increase the risk of unauthorized disclosure, disruption of critical operations, and loss of assets.

Compliance with Physical Security Policies Inadequate

Physical security controls should be designed to prevent vandalism and sabotage, theft, accidental or deliberate alteration or destruction of information or property, and unauthorized access to computing resources. These controls involve restricting physical access to computer resources, usually by limiting access to the buildings and rooms in which these resources are housed, and periodically reviewing access granted to ensure that it continues to be appropriate based on criteria established for granting such access.

FDIC has taken several actions to strengthen its physical security, including reducing the number of staff who have access to those areas where computer resources are housed. However, while it has established policies for granting access to its computer facilities and procedures for

periodically reviewing the continued need for such access, it has not yet developed a process to ensure compliance with these policies and procedures. For example, while FDIC's policy provides that contractor access may only be granted for up to 6 months, 24 of 126 contractors had access to FDIC's computer center for periods exceeding 6 months, some for several years. Without a process to ensure compliance with established policies and procedures, FDIC cannot ensure that physical access to critical computer resources is adequately controlled.

In response to our finding, the acting CIO, has since established additional controls to ensure compliance with its physical access policies relating to length of time access may be granted and maintenance of authorized access request forms. Further, FDIC recently filled a position whose duties specifically include providing daily compliance, monitoring, and oversight to ensure that physical access policies and procedures are properly followed.

Application Change Control Not Sufficient

Standard application software change control practices prescribe that only authorized, fully tested, and reviewed changes should be placed in operation. Further, these practices provide a process for reviewing all software modifications made. This should include reviews of changes made to software used to link applications to computer data and programs needed to support their operations.

While FDIC has implemented a procedure to review application software changes for evidence of unauthorized code, fraud, or other inappropriate actions, the procedure does not include a review of other types of changes, such as those made to software used to facilitate access to software files and data. As a result, unauthorized changes could be made that alter computer program logic.

In response, FDIC has expanded its application software change process to include reviews of other software modifications, including those that facilitate access to files and data.

Service Continuity Incomplete

Service continuity controls should be designed to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed, and critical and sensitive data are protected. An essential element is up-to-date, detailed, and fully tested service and business continuity plans. To be effective, these plans should be understood by all key staff and to include surprise testing.

FDIC has acted to enhance its service continuity program. For example, it (1) updated and conducted tests of its service continuity plan, (2) completed business continuity plans for all its facilities and conducted tests of these plans, and (3) established an alternate backup site to support its network and other computing resources. However, FDIC has not yet performed unannounced testing of its business continuity plan. Such tests are more realistic than announced tests and more accurately measure the readiness of staff for emergency situations. Further, FDIC had not ensured that the emergency personnel lists included in its business continuity plan are current. We identified 66 FDIC employees whose names were in the emergency personnel list but who had separated from FDIC, including 13 staff listed as key emergency team members. Without current emergency personnel lists, FDIC risks not being able to restore its critical business operations in a timely manner. FDIC has since established new procedures to ensure that emergency personnel lists remain current.

FDIC officials said that they would incorporate unannounced testing of the business continuity plan into the 2003 operating plan, and would conduct these unannounced tests by December 31 of this year.

Computer Security Program Enhanced, but Full Implementation Not Yet Achieved

The primary reason for FDIC's continuing weaknesses in information system controls is that it has not yet fully developed and implemented a comprehensive corporate program to manage computer security. As described in our May 1998 study of security management best practices,[9] a comprehensive computer security management program requires the following five elements, all essential to ensuring that information system controls work effectively on a continuing basis:

- a central security management structure with clearly defined roles and responsibilities;
- appropriate policies, procedures, and technical standards;
- security awareness;
- periodic risk assessment; and

[9]GAO/AIMD-98-68.

- an ongoing program of testing and evaluation of the effectiveness of policies and controls.

We previously recommended to FDIC that it fully develop and implement a comprehensive security management program that includes each of these elements.[10] FDIC has made progress in implementing a security management program. Specifically, it (1) established a central security management structure; (2) implemented security policies, procedures, and technical standards; and (3) enhanced security awareness training. However, the steps taken to address periodic risk assessment and ongoing testing and evaluation of policies and controls have not yet been sufficient to ensure continuing success.

Central security management structure. FDIC has established a central security function and has appointed information security managers for each of its divisions, with defined roles and responsibilities. Further, it has provided guidance to ensure that security managers coordinate with the central security function on security-related issues. It has also developed the support of divisional senior management for the central security function.

Appropriate policies, procedures, and technical standards. FDIC has updated its security policies and procedures to cover all aspects of the organization's interconnected environment and all computing platforms. It has also established technical security standards for its mainframe and network systems and security software.

Security awareness. Computer attacks and security breakdowns often occur because computer users fail to take appropriate security measures. FDIC has enhanced its security awareness program, which all employees and contractors are required to complete annually. It has also developed specialized security awareness training to address the specific needs of its security managers.

Periodic risk assessment. Regular assessments, assist management in making decisions on necessary controls by helping to ensure that security resources are effectively distributed to minimize potential loss. And by increasing awareness of risks, these assessments generate support for the adopted policies and controls, which helps ensure that the policies and

[10]GAO-02-689.

controls operate as intended. Further, *Office of Management and Budget Circular A-130*, appendix III, prescribes that risk be assessed when significant changes are made to the system but at least every 3 years.

FDIC has not fully developed a framework for assessing and managing risk on a continuing basis. While it has taken some action, including developing a framework of assessing risk when significant changes are made to computer systems and providing tools for its security managers to use in conducting risk assessments, it has not developed a process for conducting these assessments. Our study of risk assessment best practices[11] found that a process for performing such assessments should specify (1) how the assessments should be initiated and conducted, (2) who should participate, (3) how disagreements should be resolved, (4) what approvals are needed, and (5) how these assessments should be documented and maintained. In response, FDIC's acting CIO said that the corporation is taking steps to develop risk assessment guidance.

Testing and evaluation. A program that assesses the effectiveness of policies and controls includes processes for monitoring compliance with established information system control policies and procedures and testing the effectiveness of those controls. During the past year, FDIC has taken steps to establish such a program of testing and evaluation. Specifically, it has established a self-assessment program to evaluate information system controls and has implemented a program to monitor compliance with established policies and procedures that includes performing periodic reviews of system settings and tests of user passwords.

Nonetheless, FDIC's program does not cover all critical evaluation areas. Missing is an ongoing program that targets the key control areas of physical and logical access, segregation of duties, system and application software, and service continuity. In response, FDIC's acting CIO said that the corporation is taking steps to establish an oversight program to cover its control environment that will include steps to assess areas such as access controls, segregation of duties, system and application software, and service continuity. Further, FDIC plans to address each of these areas as part of its evolving self-assessment process. Until a comprehensive program to monitor and test each of these control areas is in place, FDIC will not have the oversight needed to ensure that many of the same type of

[11]U.S. General Accounting Office, *Information Security Risk Assessment: Practices of Leading Organizations*, GAO/AIMD-00-33 (Washington, D.C.: Nov. 1, 1999).

information system control weaknesses previously identified are not repeated.

An effective ongoing comprehensive program to monitor compliance with established procedures can be used to identify and correct information security weaknesses, such as those discussed in this report. For example, a comprehensive process to review all access authority granted to each user to ensure that access was limited to that needed to complete job responsibilities could identify inappropriate access authority granted to users.

A comprehensive program to regularly test information system controls can be used to detect network security weaknesses. For example, our technical reviews of network servers identified default system passwords in use that are readily known to hackers and could be used by them to gain the access needed to exploit the network and launch an attack on FDIC systems. Appropriate technical reviews of the network servers and routers can identify these types of exposures.

Conclusions

FDIC has made progress in correcting information system control weaknesses and implementing controls, including limiting and reducing access, altering software change procedures, expanding testing of disaster recovery plans, and defining the roles and responsibilities of information security officers. Nonetheless, continuing and newly identified security weaknesses exist. FDIC has not adequately restricted mainframe access, sufficiently secured its network, or completed a program for fully monitoring access activity. Weaknesses in physical security, application software, and service continuity increase the level of risk. The effect of these weaknesses—including prior and current year—further increases the risk of unauthorized disclosure of critical financial and sensitive personnel and bank examination information, disruption of critical financial operations, and loss of assets. Implementation of FDIC's plan to correct these weaknesses is essential to establish an effective information system control environment.

The primary reason for FDIC's continuing weaknesses in information system controls is that it has not yet been able to fully develop and implement a comprehensive program to manage computer security. While it has made progress in the past year in establishing key elements of this program—including a security management structure, security policies and procedures, and promoting security awareness—its systems will remain at

heightened risk until FDIC establishes a process for assessing and managing risks on a continuing basis and fully implements a comprehensive, ongoing program of testing and evaluation to ensure policies and controls are appropriate and effective. 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 are adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

Recommendations for Executive Action

To establish an effective information system control environment, in addition to completing actions to resolve prior year weaknesses that remain open, we recommend that the Chairman instruct the acting CIO, as the corporation's key official for computer security, to ensure that the following actions are completed.

- Correcting the 29 information system control weaknesses related to mainframe access, network security, access monitoring, physical access, application software, and service continuity identified in our current (calendar year 2002) audit. 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.

- Fully develop and implement a computer security management program. Specifically, this would include (1) developing and implementing a process for performing risk assessments and (2) establishing an effective ongoing program of tests and evaluations to ensure that policies and controls are appropriate and effective.

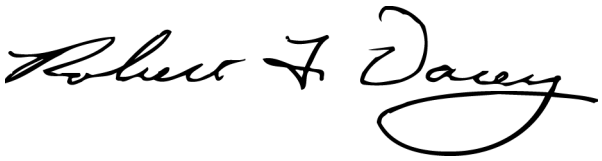
Agency Comments

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 systems control weaknesses identified and fully develop and implement a computer security management program by December 31, 2003. 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 others 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.

Sincerely yours,



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 30, 2003

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

Dear Mr. Willemssen:

Thank you for the opportunity to respond to the draft reports entitled, FDIC Information Security Progress Made But Existing Weaknesses Place Data at Risk, dated May 15, 2003. While recognizing that FDIC has made progress in correcting the information security weaknesses previously identified and has taken other steps to improve security, the General Accounting Office (GAO) did identify internal control matters in the areas of access controls, application software (change control), system software, and service continuity. These weaknesses were characterized as being the result of FDIC not having fully developed and implemented a comprehensive corporate program to manage security. We appreciate the detailed information technology audit work completed by the GAO team. We believe that it 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 report. In response to the recommendations for executive action, the FDIC will, by December 31, 2003:

- Complete corrective action for the control weaknesses identified in the 2001 review;
- Correct the 29 information systems control weaknesses identified in this year's review; and
- Fully develop and implement a computer security management program including (1) developing and implementing a process for performing risk assessments and (2) establishing an effective ongoing self-assessment program of tests and evaluations to ensure that policies and controls are appropriate and effective.

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 through substantial resources and strong executive involvement, a sustained effort is needed to address both well documented security risks and the multitude of new vulnerabilities posed by the rapidly changing technology industry. To that end, the FDIC remains committed to establishing

and improving every aspect of our corporate-wide security program. As we progress through our 2003 corrective action plans, we look forward to continuing our productive dialogue with the GAO.

If you have questions relating to the management responses, please contact Corinne Watts, Acting Director, Office of Internal Control Management, at 202-736-0076.

Sincerely,

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

cc: John Bovenzi
John Brennan
Corinne Watts
Vijay G. Deshpande
Audit Committee

GAO Contact and Staff Acknowledgments

GAO Contact

David W. Irvin, (214) 777-5716

Acknowledgments

In addition to the person named above, Edward Alexander, Gerald Barnes, Angela Bell, Nicole Carpenter, Lon Chin, Debra Conner, Anh Dang, Kristi Dorsey, Denise Fitzpatrick, David Hayes, Jeffrey Knott, Harold Lewis, Duc Ngo, Eugene Stevens, 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 GAO Mailing Lists" under "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