United States General Accounting Office

GAO

Report to the Board of Directors, Federal Deposit Insurance Corporation

July 2002

FDIC INFORMATION SECURITY

Improvements Made but Weaknesses Remain

GAO-02-689

Contents

G A O
Accountability * Integrity * Reliability

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

July 15, 2002

To the Board of Directors
Federal Deposit Insurance Corporation

We reviewed information systems general controls[1] in connection with our calendar year 2001 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.[2] 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. Our evaluation included a follow-up review of the information security weaknesses identified at FDIC in our financial statement audits for calendar year 2000.[3]

This report summarizes weaknesses in information systems controls over FDIC's computer systems. 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.

Results in Brief

FDIC made progress in correcting the information security weaknesses previously identified and has taken other steps to improve security. For

[1]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.

[2]U.S. General Accounting Office, *Financial Audit: Federal Deposit Insurance Corporation's 2001 and 2000 Financial Statements*, GAO-02-633 (Washington, D.C.: May 21, 2002).

[3]U.S. General Accounting Office, *Financial Audit: Federal Deposit Insurance Corporation's 2000 and 1999 Financial Statements*, GAO-01-635 (Washington, D.C.: May 9, 2001).

example, it has limited access to critical information, tested disaster recovery plans, and established a security awareness program. Nevertheless, we identified new weaknesses in its information systems controls that affect the corporation's ability to safeguard electronic access to critical financial and other sensitive information. These weaknesses place critical FDIC financial and sensitive personnel and bank examination information at risk of unauthorized disclosure, critical financial operations at risk of disruption, and assets at risk of loss.

FDIC did not adequately limit access to data and programs by controlling mainframe access authority, providing sufficient network security, or establishing a comprehensive program to monitor access activities. Further, other information systems control weaknesses were identified that could hinder FDIC's ability to provide adequate physical security for its computer facility, appropriate segregation of computer functions, effective control of system software changes, or ensure continuity of operations.

As we have previously reported, the primary reason for FDIC's information system control weaknesses was that the corporation had not yet fully 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. While FDIC has implemented a security awareness program, updated its security policies and guidance, and taken other actions to improve security management, it has not fully addressed all key elements of a computer security management program. These elements include (1) clearly defined roles and responsibilities for its corporate information security managers and guidance for coordinating and collaborating with central security, (2) an ongoing risk assessment process to determine computer security needs, (3) technical security standards for all computer platforms, and (4) an ongoing program of tests and evaluations to ensure that policies and controls are appropriate and effective.

To improve information system controls over FDIC financial operations, we are recommending that FDIC correct the security weaknesses identified and take additional actions to fully implement an effective corporate computer security management program. The acting chief information officer (CIO) stated that she has agreed to correct the identified weaknesses and act to fully implement such a program. The acting CIO's comprehensive corrective action plan to address each weakness will, she

said, be completed by December 31 of this year. We will evaluate the effectiveness of these corrective actions during our 2002 financial statement audits.

In providing written comments on a draft of this report, the Acting Chief Financial Officer of FDIC 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. In 1989 the Financial Institutions Reform, Recovery, and Enforcement Act was enacted 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 institution failures. The act also created the FSLIC Resolution Fund to finalize 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 $3.2 trillion for about 10,000 institutions. Together the three funds have about $49 billion in assets. FDIC had a budget of about $1.2 billion for calendar year 2001 to support its activities in managing the three funds. For that year, it processed more than 2.7 million financial transactions.

FDIC relies extensively on computerized systems to support its financial operations and store the sensitive information it collects. These systems are interconnected by FDIC's local and wide area networks. 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 supports other systems that maintain personnel information on its employees, examination data on selected financial institutions, and legal information on closed institutions. At the time of our review, there were about 5,400 authorized users on FDIC's systems.

Objective, Scope, and Methodology

Our objective was to evaluate the effectiveness of information systems general controls over the financial systems maintained and operated by FDIC during our 2001 financial statement audits.[4] These information systems 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.

Specifically, we evaluated information systems controls intended to

- protect data and application programs 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 FDIC's policies and procedures, conducted tests and observations of controls in operation, and held discussions with FDIC staff to determine whether information systems controls were in place, adequately designed, and operating effectively. In addition, we reviewed corrective actions taken by FDIC to address vulnerabilities identified in our calendar year 2000 audit. Our evaluation was based on (1) our *Federal Information System Controls Audit Manual*, which contains guidance for reviewing information systems controls that affect the integrity, confidentiality, and availability of computerized data; and (2) our May 1998 report[5] on security management best practices at leading organizations, which identifies key elements of an effective information security program.

[4]GAO-02-633.

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

We performed our work at FDIC from October 2001 through April 2002. Our work was performed in accordance with generally accepted government auditing standards.

Security Improvements Made, but System Vulnerabilities Remain

In our audit of FDIC's calendar year 2001 financial statements,[6] we found that FDIC made progress in correcting previously identified weaknesses. For instance, in our 2000 financial statement audits,[7] we determined that FDIC had not adequately limited access of authorized users, restricted physical access to computer facilities, performed comprehensive tests of the disaster recovery plan, implemented a computer security incident response process, established a security awareness program, developed security plans, and performed independent security reviews. These weaknesses placed critical corporation operations, such as financial management, personnel, and other operations, at greater risk of misuse and disruption.

Except for actions still needed to fully implement a computer security management program, which are discussed later in this report, FDIC made progress in addressing our previously reported computer security weaknesses. For example, in our 2001 audits, we found that FDIC has

- limited access of its system programmers and security staff to certain critical resources;
- developed corporate access authorization procedures;
- restricted modem connections and use of generic log on IDs to its network;
- improved physical security to its computer center by limiting access through the adjoining FDIC hotel;
- developed and performed tests of its computer center disaster recovery plans, including its network and designated remote facilities, to provide backup support for the corporation's network and other operations;

[6]GAO-02-633.

[7]GAO-01-635.

- established a computer security awareness program for its employees and contractors;

- developed security plans for its general support systems and applications; and

- implemented a requirement and process for independent security reviews to be performed at least every 3 years.

In addition to correcting previously identified weaknesses, FDIC initiated other steps to improve computer security. These efforts included (1) reviews of system software, (2) improvements in physical security, including the use of guard service to provide security surveillance to its computer rooms, (3) completed management authorizations for major financial applications and general support systems, and (4) assessments of the sensitivity of corporate data to determine the level of security needed to protect it.

However, we found additional control weaknesses in FDIC's information systems in connection with our calendar year 2001 financial statement audits. Specifically, FDIC has not adequately limited access to data and programs by controlling mainframe access authority, providing sufficient network security, or establishing a comprehensive program to monitor access activities. Other information system control weaknesses were also identified that could likewise hinder FDIC's ability to provide adequate physical security for its computer facility, appropriate segregation of computer functions, effective control of system software changes, or ensure continuity of operations. Consequently, financial, and personnel programs and data maintained by FDIC are at risk of inadvertent or deliberate misuse, fraudulent use, and unauthorized alteration or destruction, which may occur without detection.

The following sections summarize the results of our review. A separate report designated for "Limited Official Use Only" 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 planned work at FDIC.

Access to Data and Programs Was Not Adequately Controlled

A basic management control objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modifications, 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. In addition, effective network security controls should be established to authenticate local and remote users and include a program to monitor the access activities of the network and mainframe systems.

Although progress was made in limiting access, FDIC's information systems controls were not adequately protecting financial and sensitive information. Specifically, FDIC had not appropriately limited mainframe access authority, sufficiently secured its network, or established a comprehensive program to monitor access activities. These weaknesses place the corporation's information systems at risk of unauthorized access, which could lead to the improper disclosure, modification, or deletion of sensitive information and the disruption of critical operations.

Mainframe Access Authority Was Not Appropriately Limited for All Users

Effective mainframe access controls should be designed to prevent, limit, and detect access to computer programs and data. 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, we identified instances in which the corporation had not sufficiently restricted access to legitimate users. A key weakness in FDIC's controls was that its data center did not sufficiently restrict user access, as described below.

- Hundreds of users had access privileges that allowed them to modify financial software and read, modify, or copy financial data. This risk was further heightened because the corporation was not actively monitoring the access activities of these users.

- Many users had unnecessary access to powerful commands. About 55 users had access to a specific transaction command that could be used to circumvent the security of sensitive FDIC information, including its bank examination files. These users included 26 help-desk employees

and 14 database staff, users who do not need this access to perform their daily job functions.

- About 15 users outside of the system programming function had access privileges to one sensitive system software library that is allowed to perform system functions that can be used to circumvent all security controls. Such access increases the risk that users can bypass security controls to alter or delete any computer data or programs on the system. Typically such access privileges are limited to system programmers.

- About 30 users had access to powerful operator commands that could be used to circumvent system security or compromise the operational integrity of the system. Prior to the completion of our work, the acting CIO told us that this access privilege had been removed for these users.

One reason for FDIC's user access vulnerabilities was that not all access authority granted based on job responsibility was being collectively reviewed. Instead, individual access privileges were reviewed by data owners but only to determine the appropriateness of each user's access to a data owner's resource. As a result, there was no comprehensive review to determine the appropriateness of all access granted to any one user. Such reviews would have allowed FDIC to identify and correct inappropriate access.

FDIC said that it was reviewing staff access and would limit this access to that required to carry out job responsibilities. Further, the corporation plans to develop and implement procedures to comprehensively review all access granted and ensure that access remains appropriate.

Network Security Not Sufficient

Network security controls are key to ensuring that only authorized individuals gain access to sensitive and critical agency data. 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 the system software is adequately configured to prevent users from bypassing network access controls or causing network failures.

The risks introduced by the weaknesses we identified in access controls were compounded by network security weaknesses. While FDIC had taken major steps to secure its network through the installation of a firewall and other security measures, weaknesses in the way the corporation

configured its network servers, managed user IDs and passwords, provided network services, and secured its network connectivity were nonetheless still present. As a result, financial information processed on the network is at increased risk that unauthorized modification or disclosure could occur without detection. Because of FDIC's interconnected environment, these network control weaknesses also increase the risk of unauthorized access to financial and sensitive information (such as bank examination, personnel, and financial management information) maintained on the FDIC mainframe computer. For example:

- One system had default accounts that were not removed during installation of remote access software. Information on default settings and passwords is available in vendor-supplied manuals, which are available to hackers. Other systems had dormant accounts that could be used by hackers with a lower risk of detection.

- The network had system software configuration weaknesses that could allow users to bypass access controls and gain unauthorized access to FDIC's networks or cause network system failures. For instance, certain network system configuration settings allowed unauthorized users to connect to the network without entering a valid user ID and password combination. This could allow unauthorized individuals to obtain access to system information describing the network environment, including user IDs and password information.

- Potentially dangerous services were available on several network systems. Because of the availability of these services, a greater risk exists that an unauthorized user could exploit them to gain high-level access to the system and applications, obtain information about the system, or deny system services.

Further, FDIC did not have a process in place to actively review the network connections maintained by its contractors to ensure that only authorized network access paths were being used. Such network security weaknesses increase the risk that those with malicious intent could misuse, improperly disclose, or destroy financial and other sensitive information.

In response to our findings, FDIC's acting CIO said that the corporation had developed and implemented policies and procedures to periodically review (1) user accounts on all servers to ensure that they are required and appropriately used, (2) system configuration settings for vulnerabilities,

and (3) services used on the network to ensure that only those that are needed are maintained. She further said that FDIC had taken steps to tighten network security for its contractor connections and was in the process of reviewing all new contractor connections to the network to ensure appropriate access.

Program to Monitor Access Activities Not Complete

The risks created by these access control problems were heightened because FDIC did not fully establish a comprehensive program to monitor user access. A monitoring program is essential to ensuring that unauthorized attempts to access critical program 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. Such a program is critical to ensuring that improper access to sensitive information is detected.

To effectively monitor user access, it is critical that logs of user activity be maintained for all critical system processing activities. This includes collecting and monitoring access activities on all critical systems, including mainframes, network servers, and routers. Because the volume of security information is likely to be too large to review routinely, the most effective monitoring techniques selectively target specific actions. These efforts should include provisions to identify unusual activities, such as changes to sensitive system files that were not made by system programmers, or updates to security files that were not made by security staff. A comprehensive monitoring program should, further, include an intrusion-detection system to automatically log unusual activity, provide necessary alerts, and terminate sessions when necessary.

While FDIC logged access activity for many of its systems and developed programs to target unusual or suspicious activities, it did not take sufficient steps to ensure that it was recording or monitoring the access activities of all key systems, including the following:

- Special system services on the FDIC mainframe were not being logged because the audit trail that records the access activity was not enabled. As a consequence, adverse access events may not be detected that could potentially disrupt system operations or result in information system being unavailable to the corporation.

- Logging was not enabled to monitor successful or unsuccessful attempts to access sensitive router and switch configuration files on the network. Unauthorized access to these resources could enable an intruder or unauthorized user to read or modify configuration files containing security settings such as router passwords, user names, or access control listings. With the ability to read or write to these files, a malicious user could seriously disable or disrupt network operations by taking control of the routers and switches.

While FDIC has installed and implemented a network-based intrusion-detection system to monitor for unusual or suspicious access activities, it has not yet configured the host-based system parameters so that notifications (such as e-mail and/or pager) are sent to the computer security incident response team. FDIC is in the process of testing the host-based system to determine the most appropriate parameter configuration. Without full implementation of such a system and more effective logging and monitoring of system access activities, FDIC reduces its ability to identify and investigate unusual or suspicious access to its financial and sensitive information.

According to the acting CIO, the corporation has implemented security reporting for its test environment. In addition, it established procedures to provide for system logging and review of these logs for unusual or suspicious activities. Further, FDIC plans to have its intrusion-detection system fully implemented by July 31 of this year.

Other Information System Controls Were Ineffective

In addition to the information system access controls discussed, other important controls should be in place to ensure the integrity and reliability of an organization's data. These controls include policies, procedures, and control techniques to physically protect computer resources and restrict access to sensitive information, provide appropriate segregation of duties of computer personnel, prevent unauthorized changes to system software, and ensure the continuation of computer processing operations in case of disaster. FDIC had weaknesses in each of these areas.

Physical Security Controls Insufficient

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

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

Although FDIC took measures to improve its physical perimeter security and access to its computer rooms, its process for granting and reviewing physical access to the computer center is not adequately controlled. For example, there were instances in which records of access granted to staff were not available. Further, staff who no longer required access to the computer center still retained such access. This included personnel who (1) had transferred out of computer operations, (2) no longer worked for FDIC, or (3) never or rarely visited the computer room. FDIC has neither established criteria for granting physical access to its computer center, nor developed procedures to periodically review staff access to determine continued need. Without adequate criteria and periodic review, FDIC increases the risk of unauthorized access to the corporation's systems and disruption of services.

At our request, FDIC reviewed its list of staff with access to the computer center, reducing the number of authorized staff from 270 to 227. Specifically, it determined that it had no record of access granted to 18 staff, and that access was no longer needed by 25 individuals.

According to the acting CIO, the corporation has revised its computer center access procedures to include criteria for granting and retaining access to the center, and established other procedures to provide access to information on employee reassignments and other actions that could affect the need for access to the computer center. Further, she said, the corporation has developed reports on employee access activities to further assist it in monitoring physical access to the computer center.

Computer Duties Largely but Not Always Properly Segregated

Another fundamental technique for safeguarding programs and data is to segregate the duties and responsibilities of computer personnel to reduce the risk that errors or fraud will occur and go undetected. Incompatible duties that should be separated include application and system programming, production control, database administration, computer operations, and data security. Once policies and job descriptions supporting the principles of segregation of duties have been developed, it is

important to ensure that adequate supervision is provided or mitigating controls established to provide the necessary monitoring and oversight to ensure that employees perform only those tasks that have been authorized for their job functions.

Although computer duties are generally properly segregated at FDIC, we identified instances in which duties were not adequately segregated. For example, 24 application developers were authorized to make modifications to financial programs and data that were in production. Typically, developer access is limited to program code in the development environment. While it may be appropriate at times to grant developers access to both production programs and data, it should only be done when mitigating controls have been established. However, the corporation had not established mitigating controls, such as logging and monitoring system access activities of the developers to ensure that they were performing only authorized actions.

Similarly, FDIC assigned two staff members to monitor and review the access activities on its production platforms; they were also authorized to make changes to programs and data that they were responsible for reviewing. Yet, FDIC did not provide supervisory oversight or establish other mitigating controls to ensure that these staff members performed only authorized functions. Because adequate mitigating controls had not been established in either instance, the risk is increased that FDIC financial or other sensitive information could be inadvertently or intentionally modified, or unauthorized transactions processed.

FDIC plans to enhance its system monitoring of developers by targeting logging and monitoring activities to sensitive production data and programs by December 31 of this year. Further, FDIC will augment its monitoring and review of access to its production environment by designating a security person to independently review these activities.

Development and Changes to System Software Not Completely Controlled

A standard information systems control practice is to ensure that only authorized and fully tested system software or related modifications are placed in operation. To ensure that newly developed system software or changes are needed, work as intended, and do not result in the loss of data and program integrity, the system software or changes should be documented, authorized, tested, and independently reviewed.

Strong security practices provide that a structured approach be used to control the development, review, and approval of system software exits.[8] This process includes requirements for documenting the purpose of the exit, performing a technical review of the software, and approving the implementation of this software. System software exits are used to provide installations with additional processing capabilities. These exits increase the risk of integrity exposures, since the code is usually implemented with authorized privileges that allow it to bypass security and gain access to financial programs or data.

However, we identified weaknesses in the system software development and change control process at FDIC. System software exits developed by FDIC were not adequately controlled. None of the nine locally developed system software exits maintained by FDIC were documented to reflect their purpose. Further, there was no documented evidence of review by technical management or formal approval for these exits. FDIC did not develop procedures for documenting, reviewing, or approving locally developed system software exits. Without a formally documented review and approval process, an increased risk exists that the exit will not work as intended, and could result in the loss of data or program integrity.

In addition, although FDIC established a process for system software change control and used an automated system to document changes, it did not establish procedures for performing and approving tests of system software changes or develop minimum documentation requirements for tests performed. In a sample of 20 system software changes reviewed, none had documentation of the tests performed or evidence that tests performed had been approved. As a result, the risk increases that unauthorized or not adequately tested system software could be placed into operation.

FDIC's acting CIO said that the corporation would develop a process for documenting, reviewing, and approving locally developed system software exits. Further, the corporation plans to revise its requirements for documenting system software changes, provide specific requirements for testing these changes, and establish a process, by August 31 of this year to ensure compliance.

[8]A system software exit is a software program that provides an entity with flexibility to customize processing, but it also can be used to bypass security controls.

Service Continuity Planning Incomplete

An organization must take steps to ensure that it is adequately prepared to cope with the loss of operational capability due to earthquake, fire, accident, sabotage, or any other disruption. An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested service continuity plan covering all key computer operations, and including plans for business continuity. Such a plan is critical for helping to ensure that information system operations and data, such as financial processing and related records, can be promptly restored in the event of a disaster. To ensure that it is complete and fully understood by all key staff, the service continuity plan should be tested, to include surprise tests, and the test plans and results documented to provide a basis for improvement. In addition, backup sites should be reviewed and selected on the basis of their ability to provide assurance that an organization will be able to maintain continuity of operations.

While FDIC has updated and conducted tests of its service continuity plan, improvements are still needed in some areas. Service continuity weaknesses include the following:

- The lack of unannounced tests or walk-throughs of its service continuity plan. Instead, all tests have been planned, with participants fully aware of the disaster recovery scenario. In an actual disaster, of course, there is usually little or no warning.

- The lack of a business continuity plan for all its facilities. While FDIC has implemented a plan for its Washington, D.C., facility, it has yet to implement similar plans for its suburban computer center and eight regional offices.

- The potential unavailability of one of FDIC's designated computer backup facilities. This facility is in an area that could have limited accessibility in an event like September 11, 2001.

FDIC plans to develop and implement procedures for performing unannounced walk-throughs of its disaster recovery plan by September 30, 2002, and conduct and complete tests of its business recovery plans by December 31, 2002. Further, FDIC has moved all disaster recovery hardware and software from Washington, D.C., to a regional office.

Progress Made, but Full Implementation of Computer Security Management Program Not Yet Achieved

A key reason for FDIC's continuing weaknesses in information systems controls is that it has not yet fully developed and implemented a comprehensive security management program to ensure that effective controls are established and maintained, and that computer security receives adequate attention. Our May 1998 study of security management best practices[9] determined that a comprehensive computer security management program is essential to ensuring that information system controls work effectively on a continuing basis. Specifically, an effective computer security management program includes

- establishing a central security management structure with clearly delineated security roles and responsibilities;
- performing periodic risk assessments;
- establishing appropriate policies, procedures, and technical standards;
- raising security awareness; and
- establishing an ongoing program of tests and evaluations of the effectiveness of policies and controls.

FDIC has taken action related to each of the key elements described above, including the implementation of a comprehensive security awareness program for all its employees. However, aside from security awareness, the steps taken to address the other key elements of a comprehensive computer security management program were not sufficient to ensure continuing success.

The first key element of effective computer security management is the establishment of a central security group with clearly defined roles and responsibilities. This provides overall security policy and guidance, along with the oversight to ensure compliance with established policies and procedures; further, it reviews the effectiveness of the security environment. The central security group often is supplemented by individual security staff designated to assist in the implementation and management of the organizations security program. To ensure the effectiveness of the security program, clearly defined roles and

[9]GAO/AIMD-98-68.

responsibilities for all security staff should be established, and coordination responsibilities between individual security staff and central security should be developed.

While FDIC has established a central security function and is in the process of designating information security managers for each of its divisions, it has not clearly defined these managers' roles and responsibilities. Further, FDIC has not established guidance to ensure that these managers coordinate and collaborate with the central security function in addressing security related issues. Without a formally defined and coordinated program, FDIC's computer security program risks fragmentation and the lack of a corporate focus, which is needed to adequately secure its highly interconnected computer environment.

The second key aspect of computer security management is periodic risk assessment. Regular risk 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 help ensure that the policies and controls operate as intended. Further, the Office of Management and Budget Circular A-130, appendix III, prescribes that risk be assessed when significant changes are made to the system or at least every 3 years.

FDIC has not yet fully implemented a risk assessment process. While it requires a risk-based approach to security management, to date it has focused on conducting independent security reviews of its key applications and general support systems. However, these reviews do not address certain key elements for managing risk, such as identifying, analyzing, and understanding the threats to the computer environment; determining business impact when risks are exploited; and mitigating risks in a cost-effective manner. Also, FDIC has not developed a complete framework for assessing risk when significant changes are made to a facility or its computer systems. During the past year, FDIC replaced its mainframe hardware and upgraded its mainframe operating system. Either of the changes could have introduced new vulnerabilities into FDIC's computer system thus warranting a need for a risk assessment.

A third key element of effective security management is having established policies, procedures, and technical standards governing a complete computer security program. Such policies and procedures should integrate all security aspects of an organization's interconnected environment,

including local area network, wide area network, and mainframe security. In addition, technical security standards are needed to provide a consistent control framework for each computer environment. The integration of network and mainframe security is particularly important as computer systems become more interconnected.

FDIC has completed security plans for its general support systems and major financial applications. It has also developed and implemented overall security policies and procedures for its computer environment. While it has established technical security standards for several of its network platforms and its mainframe security software, it has not developed technical security standards for implementing network routers and maintaining operating system integrity on its mainframe system. Such standards would not only help ensure that appropriate computer controls are established consistently for these systems, but would also facilitate periodic reviews of the controls.

A fourth key area of security management is promoting security awareness. Computer attacks and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital that employees who use computer systems in their day-to-day operations be aware of the importance and sensitivity of the information they handle, as well as the business and legal reasons for maintaining confidentiality and integrity. In accepting responsibility for security, employees should, for example, devise effective passwords, change them frequently, and protect them from disclosure. In addition, employees should help maintain physical security over their assigned areas.

FDIC has established a comprehensive security awareness program for all employees. Specifically, it developed a computer-based security awareness program that all employees were required to complete annually. FDIC has also established procedures to monitor compliance with this requirement.

The final key area of an overall computer security management program is an ongoing program of tests and evaluations of the effectiveness of policies and controls. Such a program includes processes for (1) monitoring compliance with established information system control policies and procedures, (2) testing the effectiveness of information system controls, and (3) improving information system controls based on the results of these activities.

While FDIC established an independent security program to review compliance with application and general support system security plans on a 3-year cycle, it has not established a program to routinely monitor and test the effectiveness of information systems controls. Such a program would allow FDIC to ensure that policies remain appropriate and that controls accomplish their intended purpose.

Monitoring is key. Weaknesses discussed in this report could have been identified and corrected if the corporation had been monitoring compliance with established procedures. For example, if FDIC had a process to review all access authority granted to each user to ensure that the access was limited to that needed to complete job responsibilities, it would have been able to discover and limit the inappropriate access authority granted to hundreds of users, as discussed in this report.

A program to regularly test information systems controls would also have allowed FDIC to detect additional network security weaknesses. For example, using network analysis software designed to detect network vulnerabilities, we identified user accounts and services that could provide hackers with information to exploit the network and launch an attack on FDIC systems. Corporation staff could have identified this exposure using similar network analysis software already available to them.

In response, FDIC's acting CIO said that the corporation would develop policies and procedures to define the roles and responsibilities of its information security managers. These procedures would include requirements for coordinating security activities with the central security function. In addition, the corporation is updating its risk management directive to address the need to perform periodic risk assessments and to conduct these assessments when significant changes occur. FDIC also intends to develop and implement technical security standards for its mainframe operating system and network routers. In addition, it expects to develop and implement an ongoing security oversight program to include provisions for monitoring compliance with established procedures and testing the effectiveness of the corporation's controls. All of these initiatives are expected to be completed no later than December 31 of this year.

Conclusions

While FDIC has made progress in correcting previously identified computer security weaknesses, additional ones have been identified in its information systems control environment. Specifically, FDIC had not

appropriately limited user access authority, sufficiently secured its network, or established a program to monitor access activity. Also, FDIC was not adequately providing physical security, segregating computer duties, controlling system software, or ensuring that all aspects of its service continuity needs were addressed. Such weaknesses place sensitive FDIC information at risk of disclosure, financial operations at risk of disruption, and assets at risk of loss.

A primary reason for FDIC's information systems control problems is that it has not yet fully implemented a comprehensive program to manage computer security. While FDIC has clearly taken steps in many of these areas, more remains to be done. A comprehensive program for computer security management is essential for achieving an effective information system general control environment. Effective implementation of such a program provides for (1) periodically assessing risks; (2) implementing effective controls for restricting access based on job requirements and proactively reviewing access activities; (3) communicating the established policies and controls to those who are responsible for their implementation; and, perhaps most important, (4) evaluating the effectiveness of policies and controls to ensure that they remain appropriate and accomplish their intended purpose.

Recommendations for Executive Action

To establish an effective information systems control environment, we recommend that you instruct the acting CIO, as the corporation's key official responsible for computer security, to ensure that the following actions are completed.

- Correct the information systems control weaknesses related to access authority, network security, access monitoring, physical access, segregation of duties, system software, service continuity, and security management. These specific weaknesses are described in a separate report designated for "Limited Official Use Only," also issued today.

- Fully develop and implement a computer security management program. Specifically, this would include (1) establishing clearly defined roles and responsibilities for FDIC's information security managers and guidance for coordinating and collaborating with central security, (2) developing a program for performing periodic risk assessments to determine computer security needs, (3) developing and implementing technical security standards for all computer platforms,

and (4) establishing an ongoing program of tests and evaluations to ensure that policies and controls are appropriate and effective.

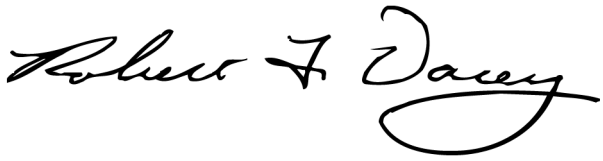
In addition, we recommend that you instruct the acting CIO to report periodically to you, or your designee, on progress in implementing FDIC's corrective action plans.

Agency Comments

In providing written comments on a draft of this report, the Acting Chief Financial Officer of FDIC agreed with our recommendations. His comments are reprinted in appendix I of this report. He reported that significant progress has already been made in addressing the weaknesses identified. Specifically, FDIC plans to correct the information systems control weaknesses related to access authority, network security access monitoring, physical access, segregation of duties, systems software, service continuity, and security management by December 31, 2002.

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; the members of the FDIC Audit Committee; officials in FDIC's divisions of information resources management, administration, and finance; and the FDIC inspector general. We will also make copies available to others upon request. In addition, the 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
801 17th Street, NW, Washington D.C. 20434

Office of the Director, Division of Finance
& Acting Chief Financial Officer

June 17, 2002

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 Improvements Made But Weaknesses Remain,* dated June 5, 2002. 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 five areas: corporate-wide security program, access controls, segregation of duties, service continuity, and systems software. 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 information security program.

Overall, the FDIC agrees with the results represented in the referenced draft reports. Specifically, in response to the recommendations for executive action, the FDIC will, by December 31, 2002, correct the information systems control weaknesses related to access authority, network security access monitoring, physical access, segregation of duties, systems software, service continuity, and security management. Specific corrective actions to be taken were provided separately.

The corrective actions include:

(1) establishing clearly defined roles and responsibilities for FDIC's information security managers and guidance for coordinating and collaborating with central security.

(2) developing a program for performing periodic risk assessments to determine computer security needs.

(3) developing and implementing technical security standards for all computer platforms.

(4) establishing an ongoing program of tests and evaluations to ensure that policies and controls are appropriate and effective.

In addition, the Chief Information Officer and the Director of Internal Control Management will periodically report to the Chief Operating Officer on the progress made on implementing corrective action plans.

We are pleased to report that significant progress has already been made in addressing the weaknesses identified in the draft reports. Further, 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 2002 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 Vijay G. Deshpande, Director, Office of Internal Control Management, at 202-736-3014.

Sincerely,

Fred Selby, Director of Finance
& Acting Chief Financial Officer

cc: Carol Heindel
Vijay Deshpande
James D. Collins

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, Nicole Carpenter, Lon Chin, West Coile, Debra Conner, Kristi Dorsey, Denise Fitzpatrick, Edward Glagola, Brian Howe, Jeffrey Knott, Harold Lewis, Suzanne Lightman, Duc Ngo, Tracy Pierson, Rosanna Villa, and Charles Vrabel made key contributions to this report.

GAO's Mission

The General Accounting Office, the 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 daily E-mail alert for newly released products" under the GAO Reports 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