GAO

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

Accounting and Information
Management Division

B-272986

September 11, 1996

The Honorable Ricki Helfer
Chairman, Board of Directors
Federal Deposit Insurance Corporation

Dear Madam Chairman:

In July 1996, we issued our opinions on the calendar year 1995 financial statements of the Bank Insurance Fund (BIF), Savings Association Insurance Fund (SAIF), and FSLIC Resolution Fund (FRF). We also issued our opinion on the Federal Deposit Insurance Corporation (FDIC) management's assertions regarding its system of internal controls at December 31, 1995, and reported on FDIC's compliance with significant provisions of selected laws and regulations for the three funds for the year ended December 31, 1995 (GAO/AIMD-96-89, July 15, 1996). In addition, we communicated several additional matters to you concerning data processing security in separate correspondence because of their sensitive nature (GAO/AIMD-96-137R, July 30, 1996).

In conducting our 1995 audits, we found that FDIC made progress in addressing some of the accounting procedure and internal control matters identified in our management letter from our 1994 audits (GAO/AIMD-95-137ML, June 5, 1995). The purpose of this letter is to report to you matters identified during our 1995 audits regarding accounting procedures and internal controls that could be improved. These matters are not considered material in relation to the financial statements of the three funds, however, we believe they warrant management's attention. We have grouped these matters into the following broad issues: disbursements (enclosure I), electronic data processing (enclosure II), and other (enclosure III). The enclosures discuss these matters and include our suggestions for improvement.

We have discussed these matters with your staff and provided a draft of this letter to your staff for comment. Your staff are in general agreement with the issues discussed in this letter. We have incorporated comments from your staff, where appropriate, particularly with respect to actions FDIC has stated it has taken, or intends to take to

157454

address these internal control issues in response to our suggestions. We will follow-up on these actions as part of our 1996 financial audits.

We conducted our 1995 financial audits pursuant to the provisions of section 17(d) of the Federal Deposit Insurance Act, as amended (12 U.S.C. 1827(d)), and in accordance with generally accepted government auditing standards.

We are sending copies of this letter to the Chairman and the members of the Audit Committee, Federal Deposit Insurance Corporation; the Chief Financial Officer, Federal Deposit Insurance Corporation; the Chief Operating Officer, Federal Deposit Insurance Corporation; the Inspector General, Federal Deposit Insurance Corporation; the Directors and Acting Directors of the Divisions of Finance, Information Resources Management, Depositor and Asset Services, Resolutions, and Administration, Federal Deposit Insurance Corporation; the Director, Office of Internal Control Management, Federal Deposit Insurance Corporation; and other interested parties.

We would appreciate receiving a description and status of your planned corrective actions within 30 days from the date of this letter. We acknowledge the cooperation and assistance provided by FDIC officials and staff during our 1995 audits. If you have any questions or need assistance in addressing these matters, please contact me at (202) 512-9406 or Steven J. Sebastian, Assistant Director, at (202) 512-9521.

Sincerely yours,

Robert W. Gramling

Robert W. Gramling
Director, Corporate Audits
and Standards

Enclosures

DISBURSEMENTS ISSUES

DISBURSEMENT AUTHORITY WAS EXCEEDED AND NOT DETECTED

The Comptroller General's Standards for Internal Controls in the Federal Government requires that transactions be authorized and executed only by persons acting within the scope of their authority. Also, FDIC's Board Resolution for the Corporate Delegations of Authority grants authority to division and office directors to approve disbursements within specified dollar limits. Further, FDIC's procedures require review of disbursement approvals to ensure that authority is not exceeded.

During our 1995 audits, we identified two disbursements in which the approving officials exceeded their delegation of authority. FDIC personnel responsible for reviewing disbursement transactions failed to detect that these officials had exceeded their authority. Inadequate transaction authorization controls, such as insufficient reviews of disbursement approvals, could result in unauthorized disbursements.

We suggest that FDIC ensure that disbursements are properly approved by stressing to division and office directors the importance of adhering to approved delegations of authority and by strengthening reviews of disbursement authorizations to detect unauthorized approvals.

In commenting on a draft of this letter, FDIC officials acknowledged the condition noted above and indicated a number of actions FDIC is taking to prevent a recurrence of the condition. Specifically, these officials stated that the Division of Finance (DOF) is emphasizing the significance and requirements of delegations of authority for all non-procurement related disbursements with disbursement operations personnel. In addition, FDIC officials stated that DOF and the Division of Administration (DOA) are conducting a joint review of invoice processing requirements and anticipate shortly issuing a memorandum to all division and offices that will address the requirements for invoice processing. FDIC officials have indicated that this memorandum will stress the importance of adhering to approved delegations of authority. We will review the status of FDIC's corrective actions as part of our 1996 financial audits.

CONTROLS OVER TRAVEL EXPENSES ARE INADEQUATE

The Comptroller General's Standards for Internal Controls in the Federal Government specifies that key duties and responsibilities for authorizing, processing, recording, and reviewing

transactions should be separated among individuals and that internal control systems reasonably ensure that assets are safeguarded against waste, loss, unauthorized use, and misappropriation. FDIC's Regular Duty Travel Regulations specify that actual expenses for meals are to be incurred only in unique or unusual situations and that adequate documentation be provided to support these expenses. In addition, FDIC has procedures requiring audits of travel expense vouchers.

During our 1995 audits, we found that (1) an FDIC official authorized his own travel, (2) duplicate payments were made for the same travel expenses, and (3) a claim for actual meal expenses was not supported by adequate documentation. FDIC's audits of travel expense vouchers failed to detect these exceptions. Weaknesses in controls over travel authorization and the travel expense audit process could result in further unauthorized or inappropriate travel expenses being incurred and further duplicate payments being made and not detected.

We suggest that FDIC ensure that its personnel are familiar with, and adhere to, its travel authorization policies and that FDIC personnel conduct more thorough audits of travel expenses.

In commenting on a draft of this letter, FDIC officials acknowledged the conditions noted above and indicated that corrective actions had been or are being taken to address these conditions. Specifically, with regard to the individual who authorized his own travel, we were told that the appropriate division director will review this executive's travel vouchers and ensure that all future travel is properly authorized. FDIC officials noted that the duplicate payments resulted from data entry errors, that FDIC had been or will shortly be reimbursed for the payments, and that corrective action has been taken to minimize the potential for such errors in the future. FDIC officials also noted that, with regard to the lack of adequate documentation supporting the claim for actual meal expenses, travel examination staff have reminded the appropriate personnel of the requirement per its regulations for a detailed receipt for actual meal expenses. We will review the effectiveness of FDIC's corrective actions as part of our 1996 financial audits.

DISBURSEMENT REVIEW PROCEDURES WERE NOT ALWAYS FOLLOWED

FDIC's Regional Accounting Manual (RAM) requires that disbursements be properly authorized, supported by adequate documentation, and recorded in the proper general ledger account. To accomplish this, the RAM requires that Accounts Payable Unit staff initial the Cash Disbursements Journal to document that checks have been reviewed and the correct account charged. Further, FDIC's Accounts Payable Purchase Order Procedures Manual requires that a DOF approving official initial the Group Edit Report to document that disbursements have been reviewed and approved.

However, we found that FDIC's disbursement review procedures were not being followed at two FDIC service centers. For example, at one service center, we found that the Cash Disbursement Journals for disbursements related to subsidiaries were not signed or initialed to indicate that a review had been performed. At another service center, we found that a DOF approving official failed to initial the Group Edit Report to document that disbursements had been reviewed and approved. We noted a misclassified expense at this service center. The failure by service center personnel to follow FDIC's prescribed disbursement review procedures can lead to errors going undetected.

We suggest that FDIC stress to service center personnel the importance of complying with the RAM and the Accounts Payable Purchase Order Procedures Manual for performing and documenting reviews of disbursement-related reports and for ensuring that expenses are recorded in the appropriate general ledger account.

In commenting on a draft of this letter, FDIC officials acknowledged the conditions noted above and indicated that corrective action was being taken to prevent future occurrences of these conditions. Specifically, we were told that DOF headquarters officials will instruct the appropriate service center managers to reiterate to service center personnel the importance of complying with both the RAM and the Accounts Payable Purchase Order Procedures Manual. FDIC officials stated that the findings involving the Group Edit Report not being initialed by a DOF approving official and the misclassified expense were isolated instances and procedures are now in place to prevent future such occurrences. FDIC officials also advised us that service center personnel are now ensuring that all Cash Disbursements Journals are being signed or initialed by the appropriate DOF approving official. We will follow up on the status of FDIC's corrective actions as part of our 1996 financial audits.

SIGNATURE VERIFICATION SYSTEM DOES NOT ADEQUATELY LIMIT ACCESS

Sound internal controls require limiting access to and the capability of changing sensitive and critical information. Such access and capabilities should be available only on an as-needed basis.

However, during our 1995 audits, we found that DOF service center accounts payable technicians were able to edit authorization information for any service center using the Signature Verification

System (SVS).[1] DOF service center personnel informed us that they did not require the capability to edit other service centers' disbursement authorization data. Providing unneeded edit capabilities can compromise the system's data integrity.

SVS provides on demand a weekly report that identifies all data changes made to a service center's delegations of authority and signature verifications and who made them. However, most technicians do not generate this report unless they are aware that an individual's delegation of authority has changed or been terminated. Consequently, unauthorized changes made by a technician at a different service center may not be detected. SVS also provides a quarterly report that is reviewed by disbursement authority delegators; however, a 3-month review interval may not be sufficient to ensure that unauthorized changes are detected in a timely manner. Furthermore, unless the capability of changing sensitive and critical information is limited, unauthorized or inappropriate disbursements may be made.

We suggest that FDIC modify SVS access controls so that accounting technicians can only edit their respective service center's disbursement authorization data. We also suggest that FDIC require more frequent routine reviews of service center delegations of authority.

In commenting on a draft of this letter, FDIC officials acknowledged the conditions noted above, but stated that the planned consolidation of all field accounting operations into a National Finance Service Center throughout 1997 will result in all editing being performed at one location. While we agree that this consolidation will eventually resolve the conditions we identified during our 1995 audits, we believe that FDIC should act on our suggestions in the interim to minimize the risk of (1) compromise to the system's data integrity and (2) unauthorized or inappropriate disbursements being made.

---

[1]The SVS is an on-line mainframe delegation of authority and signature verification system that is used by all service centers.

EDP ISSUES

ACCESS TO FINANCIAL INFORMATION SYSTEM RESOURCES DATA FILES IS EXCESSIVE

Access to production datasets used for reporting should be determined based on an analysis of the risk of information loss. In addition, the ability to modify or update system data files should be restricted to an exception basis only. When such situations arise, emergency identifications (IDs) should be used and the use of these IDs should be logged.

However, during our 1995 audits, we found that Financial Information System (FIS) reporting data files were accessible on a global basis. We also found that some users had update (write) access to FIS data files to perform problem solving related to FIS application programs and data and that this access was not logged.

FIS reporting data files may have been globally accessible because reporting data files may not be considered as sensitive as production data files. However, modification or loss of reporting data files, which are used to generate reports for financial analysis and decision-making, could affect the accuracy and reliability of financial decisions that are made using this information. Also, providing write access to data files for all support-related functions could compromise the integrity and availability of the underlying financial records.

We suggest that FDIC perform a comprehensive risk analysis and classification of FIS data and develop access controls that are commensurate with the risk to the integrity, confidentiality, and availability of the data. We also suggest that FDIC limit access to data production files to read only. Where write access is required, we suggest using emergency IDs and implementing procedures for documenting, approving, and logging emergency IDs.

In commenting on a draft of this letter, officials in FDIC's Division of Information Resources Management (DIRM) stated that DIRM staff recently completed identifying those FIS data files requiring restrictions and have put appropriate restrictions in place. These officials also stated that DIRM staff are currently developing emergency update procedures. We will review these efforts as part of our 1996 audits.

USE OF GROUP LOGON IDS IS EXCESSIVE

Group logon IDs are at times necessary for certain functions. However, the use of group logon IDs should be limited to testing and training purposes.

During our 1995 audits, we noted that FDIC maintained 38 group logon IDs, some of which are used for routine job functions. The use of group logon IDs to perform normal day-to-day job functions reduces accountability and results in the loss of an audit trail. This, in turn, could result in unintended or unauthorized system activity that remains undetected or that cannot be related to a specific system user.

We suggest that FDIC limit the use of group logon IDs to test and training purposes. We also suggest that FDIC review all group logon IDs for appropriateness and define unique IDs where possible and necessary.

In commenting on a draft of this letter, DIRM officials stated that they have reviewed the appropriateness of group logon IDs and have restricted these IDs where possible. DIRM officials noted that, as of August 15, 1996, the number of group logon IDs had been reduced to 29 and that beginning October 1, 1996, group logon IDs will be assessed quarterly to determine if further reductions are warranted. We will review the use of group logon IDs as part of our 1996 audits.

CERTAIN SECURITY PRIVILEGES ARE STILL CONSIDERED EXCESSIVE

An essential component of the separation of responsibilities within an organization is a limit on the information available to users. Information is generally made available on a need-to-know basis.

During our 1995 audits, we found that FDIC continued to provide certain information security privileges to an excessive number of individuals. We noted similar conditions in our 1993 and 1994 audits.[2] Specifically, during our 1993 and 1994 audits, we noted that as many as 18 users had the READALL privilege to FDIC's computerized information systems. Furthermore, we found that many of these 18 individuals had not used this privilege and that those few who had only needed access to a select number of files.

READALL is a powerful privilege that allows users the ability to access and review the entire database and program directory. While these users may require limited access to review selected files, such as payroll or the general ledger, individuals should not have the complete READALL privilege. During 1995, the organization responsible for these 18 individuals reduced the number

[2]1994 Financial Statement Audit Management Letter (GAO/AIMD-95-137ML, June 5, 1995), and 1993 Financial Statement Audit Management Letter (GAO/AIMD-94-160ML, August 29, 1994).

of individuals with the READALL privilege to 15 users. However, we still consider 15 users with the READALL privilege excessive.

We suggest that FDIC further review the list of users with READALL privilege and ensure that only select personnel who have a valid business purpose are provided READALL access to specific information.

In commenting on a draft of this letter, DIRM officials stated that DIRM has restricted the READALL privilege to an as-needed basis only. These officials stated that the number of individuals with the READALL privilege had been reduced to 12, and that these 12 individuals had met DIRM's criteria for establishing READALL access. DIRM officials noted that READALL access is being reviewed monthly to ensure that access privileges are appropriate. We will review the status of DIRM's actions as part of our 1996 audits.

UNRESTRICTED SYSTEM ACCESS IS NOT APPROPRIATE

Sound general controls prohibit full access to the production environment on a routine basis. Access should only be provided on an as-needed basis and should be properly approved, documented, and monitored.

However, during our 1995 audits, we noted that five users had unrestricted system access as a result of assigning the NON-CNCL privilege to their logon ID records. The NON-CNCL privilege enables a user to access any information without being canceled for a security violation. As a result, these users have full access to the production environment and are able to modify data without being detected in a timely manner by management.

We suggest that FDIC remove the NON-CNCL privilege from the five users' logon ID records and only grant this privilege on an as-needed emergency basis with proper documentation, approval, and monitoring.

In commenting on a draft of this letter, DIRM officials stated that DIRM has reviewed access authorizations and has reduced access to a minimum. These officials noted that the current procedures require that all accesses be authorized by an appropriate individual within DIRM Security, and that DIRM Security will continuously monitor these authorizations. We will review access authorizations as part of our 1996 audits.

BETTER ADHERENCE NEEDED TO SYSTEMS DEVELOPMENT LIFE CYCLE REQUIREMENTS

A systems development life cycle (SDLC) program provides the methods and tools to design, track, test, and manage the development of new systems, and, as such, affects the quality of such systems. Adherence to a formal SDLC methodology ensures that applications are appropriately developed and that vital project development tasks or controls are not bypassed. In addition, a SDLC methodology helps ensure that appropriate controls are incorporated into application designs and that user needs and management objectives are satisfied.

During our 1995 audits, we noted that FDIC's systems development process lacked enforcement across all major financial projects. Because of varying viewpoints and attitudes on controlled system development, weaknesses existed in senior management's enforcement of policies and procedures that require all newly developed systems or enhancements to follow the requirements of a formal SDLC methodology. This could result in inadequate, inefficient, undocumented, or untested systems being placed into a production environment.

We suggest that FDIC senior management enforce agencywide adherence to FDIC's formal SDLC methodology.

In commenting on a draft of this letter, DIRM officials stated that DIRM has begun to utilize a new SDLC methodology. A formal training plan for the new SDLC methodology is currently under development, and it is anticipated that SDLC training will be available by October 1996. DIRM officials noted that this training will be provided to DIRM project managers as well as to individuals within other FDIC divisions who work on systems development efforts independently or with DIRM. We will review these planned efforts during our 1996 audits.

FDIC'S DISASTER RECOVERY PLAN NEEDS ENHANCEMENT

FDIC has a formal disaster recovery plan for its computerized information systems. This plan has a designated back-up center off-site to assist in the restoration of critical processing in the event of a disruption to FDIC's computer center located in Arlington, Virginia. However, this plan does not include a list of critical applications and the order in which they are to be restored in the event of a disaster. This condition also existed during our 1993 and 1994 audits.

In the past, DIRM management has stated that identification of critical applications and the order in which they are restored was not necessary because they expect to recover all production

applications shortly after an emergency. However, this expectation was not based on a comprehensive business impact analysis. In addition, we found that full restoration of all production applications was not technically feasible since the off-site data center does not provide all the processing and telecommunications capacity needed. DIRM is currently conducting a comprehensive business impact analysis. DIRM has also designed a program that calls for the user community to prioritize systems for restoration in the event of a disaster and is pilot testing the program with two user organizations.

As in our 1993 and 1994 audits, we also noted during our 1995 audits that FDIC does not conduct unannounced disaster recovery tests. We believe that a preplanned disaster recovery test does not provide the full benefits of unannounced testing. Unannounced tests provide the opportunity to simulate actual scenarios and enhance planned reactions to disastrous events. If a service disruption occurs, users must know in advance which applications will be available for use and the restoration period for these applications. A disruption of computer services for any appreciable period would have an unacceptable impact on many vital activities and, ultimately, FDIC's mission.

We suggest that FDIC continue with its plan to establish a comprehensive disaster recovery program based on its ongoing business impact analysis. Once the disaster recovery program is finalized, we suggest that DIRM perform unannounced disaster recovery tests in a realistic simulation mode.

In commenting on a draft of this letter, DIRM officials stated that DIRM will develop procedures for conducting unannounced tests of the disaster recovery plan and include those procedures in the plan. DIRM officials expect that a draft of these procedures will be developed and testing of these procedures conducted by October 31, 1996. In addition, DIRM officials noted that a new disaster recovery policy is expected to be issued shortly. This policy, which is based on Office of Management and Budget (OMB) Circular A-130, will outline the roles and responsibilities for both DIRM and other user organizations. We will review DIRM's efforts in these areas during our 1996 audits.

FDIC NEEDS TO ENHANCE ITS PROGRAM CHANGE CONTROL PROCESS

Management of program changes to FDIC's computerized information systems is critical for supporting data security and integrity. A centralized change control function allows an entity to enforce corporate-wide standards benefiting all program applications and users. Lack of compliance with established guidelines prohibits an organization from realizing certain objectives

and does not provide assurance that all changes are properly addressed and approved prior to production implementation.

During our 1993 and 1994 audits, we found that DIRM had yet to finalize its change management policy. Although the draft change management policy set forth certain guidelines for which adherence was expected, we noted that certain policy provisions designed to provide better standardization were not being implemented. In addition, we noted that formal policies and procedures did not exist for emergency changes made and implemented during nonbusiness hours.

During our 1995 audits, we found that DIRM finalized and issued its "DIRM Change Management Policy," which defines policies and procedures for all DIRM-managed production systems to ensure that all changes are properly approved, tested, and implemented to minimize negative impacts on the production environment. However, we found that although program changes conformed with prescribed policies and procedures at one time, compliance efforts had stopped and not all groups were utilizing the Change Control Application System (CCAS) to log change requests. For example, we found that one group reverted to using a customized means to track and manage changes. In addition, we noted that test plan developments did not adhere to guideline specifications and that changes of an emergency nature did not subsequently receive proper approval and follow-up.

If these conditions continue to remain uncorrected, there is a risk that application integrity may not be maintained. Changes may not be properly analyzed and approved if CCAS does not serve as the repository for all change information from the initial request to implementation. Also, if formal guidelines for emergency modifications are not adhered to, appropriate personnel may not be notified and emergency changes may not be properly tested.

We suggest that DIRM formally communicate the roles and responsibilities of personnel involved in the change management process and enforce adherence to change management policies and procedures. In addition, we suggest that user "after the fact" approvals be provided for all emergency change implementations.

In commenting on a draft of this letter, DIRM officials noted that DIRM is currently finalizing modifications to its formal change management policy directives. These officials noted that the modified policy directives, when reissued in late 1996, should provide for standardization of change management policies and procedures within DIRM and other divisions. We will review the status of DIRM's efforts as part of our 1996 audits.

OTHER ISSUES

POLICIES AND PROCEDURES FOR CALCULATING RESERVES ON ASSETS FROM OPEN ASSISTANCE TRANSACTIONS DO NOT EXIST

Standard polices and procedures are necessary to ensure that FDIC personnel responsible for valuing assets acquired through open assistance transactions and deriving the related loss provisions for these assets are reviewing the same documentation, operating under comparable assumptions, and following a consistent methodology.

In open assistance transactions, FDIC acquires assets, such as notes receivables and stock certificates, as a result of providing assistance to troubled institutions in an effort to avert their failure. In our 1994 audits, we noted that FDIC did not have documented policies and procedures describing how recovery values for these assets were to be established.[3] In response to our concerns, FDIC indicated that the Division of Resolutions (DOR), in close coordination with DOF, would draft specific written policies for calculating recovery values for assets acquired through open assistance transactions. However, as of the end of our 1995 audits in May 1996, FDIC still had not established written policies to estimate recovery values for open assistance-related assets. Lack of a written policy increases the risk that estimated recovery values for these assets are not based on uniform and reasonable criteria.

We suggest that FDIC develop and implement a specific written policy covering the valuation of open assistance-related assets and document a standard methodology for responsible personnel to follow in estimating recovery values for these assets.

In discussions with DOR officials in August 1996, they noted agreement with the condition discussed above. These officials stated that DOR will develop specific written policies for calculating recovery values for assets acquired through open assistance transactions, and they expect these written policies will be developed and implemented in the near future. We will follow up on FDIC's efforts as part of our 1996 audits.

---

[3]1994 Financial Statement Audit Management Letter (GAO/AIMD-95-137ML, June 5, 1995).

FDIC DEBITED INSTITUTION ACCOUNTS WITHOUT PROPER AUTHORIZATION

FDIC's policy requires that each federally-insured depository institution provide written authorization to FDIC to debit the institution's designated assessment account. These authorization letters provide to FDIC all information and authorizations needed for direct debit of the account and only need to be updated if the institution designates a different account for assessment debit. Changes must be by written notice, similar to the initial authorization letter.

During our 1995 audits we found that (1) two Routing Transit Number (RTN) authorization letters were not signed, (2) one RTN authorization letter was dated December 19, 1995, well after the direct debit, and (3) manual modifications were made to account numbers and/or RTNs on several of the RTN authorization letters. These conditions existed because FDIC lacked appropriate internal control procedures to ensure that all institutions had valid RTN authorization letters on file and that modifications of RTN letters were properly authorized by the institutions. FDIC's debiting of institution accounts without proper authorization letters on file may result in erroneous charges to member institutions.

We suggest that FDIC establish and document procedures to ensure that valid RTN authorization letters are on file for all institutions prior to any direct debit of their accounts.

In commenting on a draft of this letter, FDIC officials noted their agreement with and recognition of the importance and sensitivity of all assessments-related data and documentation. These officials noted that historically FDIC has had numerous checks and balances and control points in place to prevent erroneous debits to member institutions. However, these officials noted that FDIC is currently in the process of reviewing and reconciling the total universe of authorization letters to ensure that each letter has been properly endorsed and that there is a form letter on file for every FDIC-insured depository institution subject to assessment. We will review the status of FDIC's efforts in this area as part of our 1996 audits.

LEAST COST RESOLUTION DECISIONS WERE NOT DOCUMENTED

The FDIC Improvement Act (FDICIA) of 1991 requires FDIC to resolve failed insured financial institutions in the manner least costly to the insurance funds. FDICIA also requires that FDIC adequately document its consideration of available options and the rationale for the final selection of the resolution option to be pursued (i.e., the least cost test). In accordance with a 1992 FDIC

Board of Directors Resolution (the Robinson Resolution), the Board may delegate the least cost test and final selection of the resolution option to the DOR director or his/her designee.

During our 1995 audits, we found that in each of the three cases in 1995 in which FDIC's Board of Directors delegated the least cost test and final resolution decision to the DOR director or his/her designee, file documentation of the cost test did not contain evidence that the final resolution decision was approved by the DOR director or his/her designee prior to its implementation.

The 1992 Robinson Resolution mandates the 5-year retention of documents related to any determination and/or evaluation made by the DOR director or his/her designee in connection with the least cost test. DOR uses a checklist in the cost test files to ensure that each file contains all necessary documents. However, a document demonstrating approval of the resolution is not required by the Robinson Resolution and therefore is not a required item on this checklist. In addition, for one of the institutions resolved under the Robinson Resolution, we found that the cost test file did not contain a documentation checklist.

Failure to fully document least cost resolution decisions increases the risk that FDIC will select a resolution option that is not the least costly to the applicable insurance fund.

We suggest that DOR fully document all resolution decisions it makes on behalf of the Board of Directors. Further, we suggest that DOR modify its documentation checklist to include written approval of the resolution decision by the DOR director or his/her designee and ensure that responsible DOR staff maintain this checklist in all such files.

In commenting on a draft of this letter, DOR officials concurred with the condition noted above. These officials noted that, while not formally documented, the least cost test was performed for the three cases noted above, and in each case the final resolution decision was verbally approved by the DOR director. These officials stated that in the future, DOR will fully document all resolution decisions and the files will contain written documentation showing the name of the person approving the transaction and the date of the approval. These officials also noted that the resolution checklist is currently being modified to include an item for Robinson Resolution approvals. We will review DOR's efforts in this area as part of our 1996 audits.

(917699)

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER

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

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested