



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

Accounting and Information
Management Division

B-270426

January 18, 1996

Mr. Carl Powell
Director of Automation Resources
Federal Reserve Automation Services
701 E. Byrd St., 6th Floor
Richmond, VA 23219

Dear Mr. Powell:

As part of our response to a request by Representative Henry B. Gonzalez, we reviewed general controls¹ over the computer financial information systems maintained by the Federal Reserve Automation Services (FRAS) in Richmond, Virginia. We limited our evaluation to those FRAS computer systems which support the Federal Reserve Bank (FRB) of Dallas.

Our review identified weaknesses in the general controls over FRAS' computer systems. Addressing these matters will strengthen general controls and should improve the overall computer security environment. Corrective actions have been taken to address most of these weaknesses. The purpose of this letter is to advise you of the weaknesses we identified and their current status.

¹General controls are policies and procedures that apply to the overall effectiveness and security of an entity's computer operations and create the environment in which other related computer controls operate. General controls include the organizational structure, operating procedures, software security features, and physical protection designed to ensure that (1) only authorized changes are made to computer programs, (2) access to computer systems and data is appropriately restricted, (3) backup and recovery plans are adequate to ensure the continuity of essential operations, and (4) computer security duties are segregated.

We evaluated those FRAS computer systems which support the major financial applications of the Federal Reserve Bank of Dallas, including the Integrated Accounting System (IAS), Electronic Payment System, Check Processing system, and Automated Clearing House system. These systems are central to processing transactions which ultimately affect the Federal Reserve Bank of Dallas' financial statements. For example, the IAS processed all accounting transactions for approximately \$16 billion in assets and \$895 million in net income on the Federal Reserve Bank of Dallas' financial statements for the period ending December 31, 1994.

In performing our review, we tested and observed the operation of general controls over certain financial information systems to determine whether they were adequately designed, in place, and operating effectively. For example, with the knowledge and cooperation of FRAS, we attempted to access sensitive data and programs.

Our review was performed primarily at the FRAS computer center in Richmond, Virginia, from September 1994 to October 1995 in accordance with generally accepted government auditing standards. We have discussed the results of our review with appropriate FRAS staff, provided them a draft of this report, and have incorporated their comments where appropriate.

CORRECTIVE ACTIONS
HAVE ADDRESSED MOST
IDENTIFIED WEAKNESSES

During our review, we identified general control weaknesses in a number of areas and communicated them to the appropriate FRAS personnel. Before the review was completed, FRAS staff had taken corrective actions to address most of the concerns raised. The following summarizes these weaknesses and the corrective actions taken to address them.

Access to Sensitive Information

- Access to job management software called "Spool Display Search Facility" (SDSF) was not restricted to appropriate authorized individuals. Using SDSF, users can view, print, or redirect job output to an alternate destination of their choice. At the time of our review, all FRAS users on the computer system that supports IAS were able

to view job output for any user on the system. As a result, all users had access to potentially sensitive data on IAS. Once we brought this control weakness to the attention of FRAS staff, they corrected the system problem by modifying the software installation to limit access appropriately.

- Access to one of the Authorized Program Facility (APF) libraries was not adequately restricted or monitored. At the time of our review, 292 technical and operational support staff were allowed update access to this APF library. Further, that access to this library was not logged. Federal Reserve standards prohibit such actions because this unrestricted access might result in unauthorized changes affecting the overall integrity of the system software environment. To address our concerns, FRAS staff eliminated unnecessary update access and ensured that a log of changes to this APF library was created and would be maintained. Although this weakness was not observed for the other APF libraries, FRAS established procedures to uniformly control and monitor access to APF libraries to ensure that Federal Reserve standards are followed.
- The configuration of security software used to protect sensitive financial information did not ensure that all unauthorized access was denied. FRAS staff have modified the security software parameters to ensure that all unauthorized access is prevented. FRAS staff also initiated procedures to periodically review security software parameters to ensure that they are appropriate and consistent with Federal Reserve standards.
- FRAS had not established an audit trail to determine whether special privileges granted to users who accessed the computer system which supports IAS were authorized. Of 29 judgmentally selected FRAS users with access to the computer system which supports IAS, 15 had no documentation showing that FRAS management had authorized that access. According to FRAS Data Security staff, these privileges were associated with job functions rather than specific job duties and therefore were appropriate. Nevertheless, FRAS management responded to our concern by documenting access privileges to be assigned to all staff in specific areas and requiring a specific request and justification for additional privileges.

- Certain sensitive system files were not adequately protected from unauthorized access. These system files, known to FRAS as SYS1.UADS and SYS1.PAGEDUMP, contain computer access identification information and passwords which could allow unauthorized users to access the Federal Reserve Bank of Dallas' financial systems. FRAS changed the dataset rules to correct this.
- Emergency access identifications were not effectively controlled to ensure that their use was limited appropriately. These identifications allow the user to insert, modify, or delete virtually any financial data or related computer application program and system software. They are intended only for limited purposes, such as handling problems or emergencies that interrupt the system's 24-hour-a-day operation. During a randomly selected 1-week period, we observed that emergency identifications were used to access computer programs and data files several thousand times. To verify that this was not an isolated or one-time problem, we selected an additional 1-week period and observed that emergency identifications were used at the same level.

To correct this, FRAS implemented new software that should allow staff to make certain changes without using emergency identifications. This should enable FRAS to confine the granting of emergency identifications to the emergency situations for which they were originally intended.

Access to the Computer Center

- Physical access to the FRAS computer center was not adequately controlled for contractor personnel. We found instances where access to the computer center was inappropriately granted to contractor personnel who worked in such areas as marketing and sales that did not warrant this access. We also identified contractor personnel who had access to the computer center when such access was no longer required. This included personnel who no longer worked for the contractor and contractor personnel who did not regularly visit the computer center. At our request, FRAS staff reviewed their list of authorized contractor personnel with access to the computer center and reduced the number of authorized personnel from 174 to 104. In addition, new procedures were developed to limit the

number of contractor personnel with physical access to the computer center in the future.

Changes to System Software

-- FRAS lacked control policies and procedures for independently testing and certifying system software changes prior to their implementation. In reviewing system software changes made between January and August 1994, we found no documentation indicating that these changes had been independently tested or reviewed. At the time of our review, approximately 15 percent of FRAS system software changes had problems during or after implementation, a rate considered high by FRAS personnel. To address this concern, guidelines were developed requiring that system software changes be tested and certified prior to implementation.

CORRECTIVE ACTIONS STILL NEEDED
TO ADDRESS SOME IDENTIFIED WEAKNESSES

While corrective actions have already been completed to address most general control weaknesses we identified, other matters have not been fully addressed and still warrant management's attention. These matters are (1) fully testing the disaster recovery plan and (2) completing the review of the use of started tasks² with special privilege authority. We have discussed these matters with key members of your staff and were told that all control issues will be addressed in early 1996.

Disaster Recovery Plan
Has Not Been Fully Tested

A basic internal control objective is to establish a disaster recovery plan to ensure the continuity of data processing operations during power outages or other crises. Although FRAS had a disaster recovery plan, certain components were missing or were not current. These included the following:

²Started tasks are routines that are automatically started by the system.

- FRAS had not established a priority order for processing critical applications in the event of a disaster or procedures for determining this order.
- The disaster recovery notification list used to contact team members in the event of a disaster was not current.
- FRAS had not developed a program for conducting a periodic risk analysis of its computer installations.

Since our review, FRAS staff have completed their disaster recovery plan to include these missing items.

Internal control objectives also state that an entity's disaster recovery plan should be fully tested. Although FRAS staff had performed numerous partial tests of their disaster recovery plan, they had not conducted a complete test of the network communication system that links the FRBs, depository institutions, and FRAS computer centers. Such tests are necessary to ensure that critical operations can be continued. In addition, FRAS staff had not conducted unannounced tests of their disaster recovery plan, a scenario more likely to be encountered in the event of an actual disaster. Instead, all tests had been preplanned with participants fully aware of the disaster recovery test scenario.

Subsequent to our review, FRAS conducted an unannounced test of the disaster recovery notification procedures. FRAS plans to conduct periodic unannounced tests that will be expanded to include other aspects of the disaster recovery plan. However, FRAS staff still have not performed a complete test of their network communication system.

We suggest that FRAS staff periodically perform a complete test of the disaster recovery plan. Such testing should include not only the FRAS computer centers, but should also involve participation by the FRBs and depository institutions. According to the FRAS Disaster Recovery Manager, efforts to have depository institutions participate in a complete test of the disaster recovery plan have been incorporated in the initiatives being undertaken by the Financial Services Management Committee of the federal reserve banks. The committee plans to include depository institutions in a complete test of the disaster recovery plan.

Use of Started Tasks
With Special Privileges
Needs to Be Reviewed

A standard computer control practice is to ensure that special privileges allowing access to all information resources are appropriately limited. We found that FRAS had 258 computer programs, known as started tasks, that were granted special privileges. The privileges allow users of these programs to access virtually any financial data file or related computer application program and system software, regardless of the security protection level assigned to these resources. Because these started-task programs have such broad access to sensitive information, their number needs to be controlled.

FRAS personnel noted that the computer systems on which these started tasks reside were among the first systems migrated to the consolidated FRAS computer environment. To ensure the successful operation of the migrated systems, FRAS management agreed to allow the Federal Reserve Bank of Dallas to use special privileges on all its started tasks. FRAS staff told us that since the computer environment is now more mature, the use of started tasks with unlimited access is no longer warranted in many cases.

Since our review was completed, FRAS has, at our suggestion, already eliminated a number of started tasks with special privileges. However, started tasks with unnecessary privileges still exist. FRAS management plans to complete the clean up of the started tasks with special privileges as soon as possible.

- - - - -

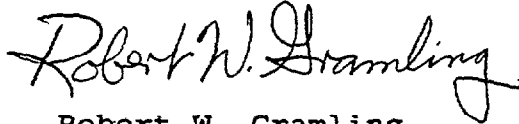
We would like to thank FRAS for the courtesy and cooperation extended to our audit team. We ask that FRAS management keep us informed of corrective actions taken on these issues.

We are sending copies of this letter to Representative Henry B. Gonzalez; the Chairman, House Committee on Banking and Financial Services; the Chairman and Ranking Minority Member of the Senate Committee on Banking, Housing and Urban Affairs; and the Chairman of the Board of Governors, Federal Reserve System.

B-270426

If you have any questions about this letter, please call me
at (202) 512-9406.

Sincerely yours,

A handwritten signature in cursive script that reads "Robert W. Gramling". The signature is written in black ink and is positioned above the typed name.

Robert W. Gramling
Director, Corporate Audits
and Standards

(917697)

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. 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

**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
