



G A O

Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

August 29, 2002

Louise L. Roseman, Director
Division of Reserve Bank Operations
and Payment Systems
Board of Governors of the Federal
Reserve System

Subject: *Federal Reserve Banks: Areas for Improvement in Computer Controls*

Dear Ms. Roseman:

In connection with fulfilling our requirement to audit the U.S. government's fiscal year 2001 financial statements, we reviewed the general and application computer controls over key financial systems maintained and operated by the Federal Reserve Banks (FRB) on behalf of the Department of the Treasury's Bureau of the Public Debt (BPD).¹ This report for public release summarizes the results of our fiscal year 2001 work, including our follow-up on previous years' recommendations.

The 12 FRBs perform fiscal agent services on behalf of the U.S. government, including BPD. The debt-related services primarily consist of issuing, servicing, and redeeming Treasury securities and processing secondary market securities transfers. Five FRB data centers maintain and operate key BPD financial applications relevant to the Schedule of Federal Debt.

We used a risk-based and rotation approach for testing general and application controls. Under that methodology, every 3 years each significant data center and each key application is subjected to a full-scope review, which includes testing in all the computer control areas defined in the *Federal Information System Controls Audit Manual* (FISCAM).² In the interim years, we focus our testing on selected control areas defined in FISCAM. We performed our work at the FRBs from September 2001 through January 2002. Our work was performed in accordance with U.S. generally accepted government auditing standards. We requested comments on a draft of this report from the Board of Governors of the Federal Reserve System. The comments are discussed later in this report and are reprinted in the enclosure.

As noted above, our review addressed both general and application controls. An effective general control environment (1) protects data, files, and programs from

¹31 U.S.C. 331(e) (2000).

²U.S. General Accounting Office, *Federal Information System Controls Audit Manual, Volume I: Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: Jan. 1999).

unauthorized access, modification, and destruction, (2) limits and monitors access to programs and files that control computer hardware and secure applications; (3) prevents the introduction of unauthorized changes to systems and applications software, (4) prevents any one individual from controlling key aspects of computer-related operations, and (5) ensures the recovery of computer processing operations in case of disaster or other unexpected interruption. An effective application control environment helps ensure that transactions performed by individual computer programs are valid, properly authorized, and completely and accurately processed and reported.

As we reported in connection with our audit of the Schedules of Federal Debt for the fiscal years ended September 30, 2001 and 2000,³ BPD maintained, in all material respects, effective internal control relevant to the Schedule of Federal Debt related to financial reporting and compliance with applicable laws and regulations as of September 30, 2001. BPD's internal control, which includes the general and application controls implemented by the FRBs over key BPD systems relevant to the Schedule of Federal Debt, provided reasonable assurance that misstatements, losses, or noncompliance material in relation to the Schedule of Federal Debt for the fiscal year ended September 30, 2001, would be prevented or detected on a timely basis.

Our follow-up on the status of the FRBs' corrective actions to address vulnerabilities identified in our audit for fiscal year 2000 found that the FRBs had corrected or mitigated the risks associated with 25 of the 29 general and application control vulnerabilities discussed in our prior report⁴ and are in the process of addressing the remaining 4.

In a separately issued Limited Official Use Only report, we communicated detailed information regarding our findings to FRB managers and made 9 recommendations to improve certain computer controls in the areas of access, system software, and service continuity. None of our findings pose significant risks to BPD financial systems. Nevertheless, they warrant FRB managers' action to further decrease the risk of inappropriate disclosure and modification of sensitive data and programs, misuse of or damage to computer resources, and disruption of critical operations.

In commenting on a draft of this report, the Board of Governors of the Federal Reserve System stated that overall it found the review helpful and that the information in the report will assist the Federal Reserve System in its ongoing efforts to enhance the integrity of its automated systems and information security practices. The board agreed with our assessment that FRBs have implemented effective computer controls and that while the vulnerabilities identified do not pose significant risks to Treasury's financial systems, they warrant FRB management's attention. The board stated that it has corrected or will correct all the vulnerabilities we identified.

³U.S. General Accounting Office, *Financial Audit: Bureau of the Public Debt's Fiscal Years 2001 and 2000 Schedules of Federal Debt*, GAO-02-354 (Washington, D.C.: Feb. 15, 2002).

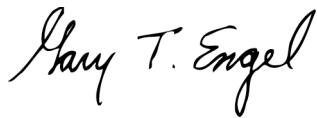
⁴U.S. General Accounting Office, *Federal Reserve Banks: Areas for Improvement in Computer Controls*, GAO-02-266R (Washington, D.C.: Dec. 2001).

We will follow up on these matters during our audit of the federal government's 2002 financial statements.

We are sending copies of this report to the Chairman and Ranking Minority Member of the Senate Committee on Governmental Affairs; Subcommittee on Treasury and General Government, Senate Committee on Appropriations; House Committee on Government Reform; and Subcommittee on Treasury, Postal Service, and General Government, House Committee on Appropriations. We are also sending copies of this report to the Chairman of the Board of Governors of the Federal Reserve System and the Director of the Office of Management and Budget. Copies will also be made available to others upon request. In addition, the report will be available at no charge on GAO's Web site at <http://www.gao.gov>.

If you have any questions regarding this report, please contact Paula M. Rascona, Assistant Director, at (202) 512-9816. Other key contributors to this assignment were Louise DiBenedetto, David B. Hayes, Greg Wilshusen, and Mickie Gray.

Sincerely yours,

A handwritten signature in cursive script that reads "Gary T. Engel".

Gary T. Engel
Director
Financial Management and Assurance

Enclosure

Comments from the Board of Governors of the Federal Reserve System



BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

LOUISE L. ROSEMAN
DIRECTOR
DIVISION OF
RESERVE BANK OPERATIONS
AND PAYMENT SYSTEMS

July 18, 2002

Mr. Gary T. Engel
Director
Financial Management and Assurance
United States General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Engel:

We appreciate the opportunity to comment on the General Accounting Office's draft report assessing the Federal Reserve Banks' information security associated with the applications that support their role as fiscal agents of the United States. The GAO's review was performed as part of the audit of the U.S. government's fiscal year 2001 financial statements.

Overall, we found the review and report helpful. The report provides information that will assist the Federal Reserve System in its ongoing efforts to enhance the integrity of its automated systems and information security practices. The Federal Reserve shares lessons learned from this review and its internal reviews with appropriate Federal Reserve staff to improve controls, processes and internal audit procedures more broadly within the System.

We agree with GAO's assessment that the Federal Reserve has implemented effective controls over these applications. We also agree with the GAO's assessment that while the vulnerabilities identified in the report do not pose significant risks to the Treasury's financial systems, they still warrant management's attention. Of the nine vulnerabilities in the report that require attention, we have corrected or will correct all of them. Federal Reserve Board staff will monitor the status of uncorrected items. Internal auditors at the Reserve Banks will confirm all corrective measures taken.

Sincerely,

A handwritten signature in cursive script that reads "Louise L. Roseman".

(198119)