



GAO

Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

May 12, 2004

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 financial statements of the U.S. government,¹ we audited and reported on the Schedules of Federal Debt Managed by the Bureau of the Public Debt (BPD) for the fiscal years ended September 30, 2003 and 2002.² As part of these audits, we performed a review of 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 BPD.

Many of the 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. In fiscal year 2003, the FRBs issued about \$4.1 trillion in federal debt securities to the public, redeemed about \$3.8 trillion of debt held by the public, and processed about \$125 billion in interest payments on debt held by the public. FRBs maintain and operate key financial applications on behalf of BPD and an array of financial and information systems to process and reconcile monies disbursed and collected on behalf of BPD.

The scope of our work for fiscal year 2003 included a review of the general and application computer controls over key financial systems maintained and operated by the FRBs on behalf of BPD and follow-up on unresolved vulnerabilities identified in prior years' audits of these systems. We use a risk-based and rotation approach for testing general computer controls. Each general control area is subjected to a full-scope review, including testing, at least once every 3 years. The computer control areas we review are defined in the *Federal Information System Controls Audit*

¹31 U.S.C. § 331(e) (2000).

²U.S. General Accounting Office, *Financial Audit: Bureau of the Public Debt's Fiscal Years 2003 and 2002 Schedules of Federal Debt*, GAO-04-177 (Washington, D.C.: Nov. 7, 2003).

*Manual.*³ Areas considered to be of higher risk are subject to more frequent review. The applications are subjected to a full-scope review every year.

General computer controls are intended to (1) protect data, files, and programs from unauthorized access, modification, disclosure, and destruction; (2) limit and monitor access to programs and files that control computer hardware and secure applications; (3) prevent the introduction of unauthorized changes to systems and applications software; and (4) ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption. Application computer controls relate directly to the individual computer programs that are used to perform certain types of work, such as generating interest payments or recording transactions in a general ledger. In an effective general control environment, application controls help to ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. Access controls for specific applications should establish individual accountability and proper segregation of duties, prevent unauthorized transactions from being entered into the application and processed by the computer, limit the processing privileges of individuals, and prevent and detect inappropriate or unauthorized activities.

We performed our work at certain FRBs from April 2003 through October 2003 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 summarized later in this report and the written response from the Board of Governors is reprinted in the enclosure.

As we reported in connection with our audit of the Schedules of Federal Debt for the fiscal years ended September 30, 2003 and 2002, BPD maintained, in all material respects, effective internal control, including general and application computer controls, relevant to the Schedule of Federal Debt related to financial reporting and compliance with applicable laws and regulations as of September 30, 2003. BPD's internal control provided reasonable assurance that misstatements, losses, or noncompliance material in relation to the Schedule of Federal Debt for the fiscal year ended September 30, 2003, would be prevented or detected on a timely basis. We found matters involving computer controls that we do not consider to be reportable conditions.⁴

In a separately issued Limited Official Use Only report, we communicated detailed information regarding our findings to FRB managers and made five recommendations that address application computer control vulnerabilities related to access controls. In addition, our follow-up on the status of the FRBs' corrective actions to address unresolved vulnerabilities identified in prior years' audits found that the FRBs had

³U.S. General Accounting Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

⁴Reportable conditions are matters coming to our attention that in our judgment should be communicated because they represent significant deficiencies in the design or operation of internal control, which could adversely affect the organization's ability to meet the objectives of reliable financial reporting and compliance with applicable laws and regulations.

taken corrective action for three of the four open recommendations discussed in our prior report.⁵ The one remaining open recommendation related to access controls is now encompassed in one of the five new detailed recommendations contained in the Limited Official Use Only report.

While the application computer control vulnerabilities reported do not pose significant risks to the financial systems maintained and operated by the FRBs on behalf of BPD, they warrant FRB managers' action to decrease the risk of unauthorized access or data misuse.

We recommend that the Director of the Division of Reserve Bank Operations and Payment Systems assign responsibility and accountability for addressing the five recommendations to cognizant FRB officials.

In commenting on a draft of this report, the Board of Governors of the Federal Reserve System stated that the information in this report and the Limited Official Use Only report will assist the FRBs in their ongoing efforts to enhance the integrity of their automated systems and information security practices. The Board of Governors also stated that the five vulnerabilities remaining as of September 30, 2003, have been or will be corrected and pledged to monitor the status of uncorrected items. We plan to follow up on these matters during our audit of the fiscal year 2004 Schedule of Federal Debt.

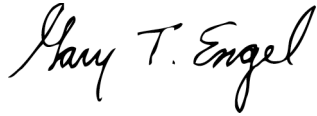
In the separately issued Limited Official Use Only report, we requested a written statement on actions taken to address these recommendations.

We are sending copies of this report to the Chairmen and Ranking Minority Members of the Senate Committee on Governmental Affairs; the Subcommittee on Transportation, Treasury and General Government, Senate Committee on Appropriations; the House Committee on Government Reform; the Subcommittee on Government Efficiency and Financial Management, House Committee on Government Reform; and the Subcommittee on Transportation and Treasury, and Independent Agencies, 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>.

⁵U.S. General Accounting Office, *Federal Reserve Banks: Areas for Improvement in Computer Controls*, GAO-03-333R (Washington, D.C.: Feb. 10, 2003).

If you have any questions regarding this report, please contact Louise DiBenedetto, Assistant Director, at (202) 512-6921. Other key contributors to this assignment were Gerald L. Barnes, Dean D. Carpenter, Mickie E. Gray, David B. Hayes, and Dawn B. Simpson.

Sincerely yours,

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

Gary T. Engel
Director
Financial Management and Assurance

Enclosure

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

March 18, 2004

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 2003 financial statements.

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

We agree with GAO's assessment that the Reserve Banks have 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 five 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 and internal auditors at the Reserve Banks will confirm all corrective measures taken.

Sincerely,

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

(198257)