United States General Accounting Office

GAO

Report to the Secretary of the Treasury

October 1998

BUREAU OF THE PUBLIC DEBT

Areas for Improvement in Computer Controls

GAO/AIMD-99-2

GAO

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

Accounting and Information
Management Division

B-280813

October 14, 1998

The Honorable Robert E. Rubin
The Secretary of the Treasury

Dear Mr. Secretary:

We recently reported on the U.S. government's consolidated financial statements (GAO/AIMD-98-127, March 31, 1998) and the Bureau of the Public Debt's (BPD) Schedule of Federal Debt (GAO/AIMD-98-65, February 27, 1998) for fiscal year 1997. These audits were conducted under the Chief Financial Officers (CFO) Act of 1990, as expanded by the Government Management Reform Act of 1994 (GMRA). Our review of the general and application computer controls over key BPD financial systems was performed as part of these audits. On July 31, 1998, we issued a "Limited Official Use" report to you detailing the results of our review. This version of the excerpted report for public release provides a general summary of the vulnerabilities we identified and the recommendations we made.

This report discusses general and application controls that support key automated financial systems maintained and operated by BPD. These systems process investments and redemptions of Treasury securities, generate interest payments, account for the resulting debt, and provide financial reports to the public and the federal government.

General controls affect the overall effectiveness and security of a computer processing facility as opposed to being unique to any specific computer application processed there. They are intended to (1) protect data, files, and programs from unauthorized access, modification, and destruction, (2) prevent the introduction of unauthorized changes to systems and applications software, (3) ensure that system software development and maintenance, applications software development and maintenance, computer operations, security, and quality assurance functions are performed by different people, (4) ensure recovery of computer processing operations in case of a disaster or other unexpected interruption, and (5) ensure that an adequate computer security planning and management program is in place.

Application controls are the structure, policies, and procedures that apply to individual application systems. These controls help to ensure that transactions are valid; properly authorized; and completely, promptly, and accurately processed by the computer.

As we reported in connection with our audit of the Schedule of Federal Debt, management of BPD fairly stated that its related internal controls, including computer controls, were effective. However, as discussed in this report, we found vulnerabilities involving computer controls that we did not consider reportable conditions,[1] but, if left uncorrected, could increase the risk of inappropriate disclosure and modification of sensitive information, misuse or damage of computer resources, and disruption of critical operations. These vulnerabilities warrant management's attention and action. While performing our work, we communicated our interim findings and recommended corrective actions for each specific finding to BPD management. This report summarizes those findings.

Results in Brief

Overall, we found that BPD implemented effective computer controls; however, we identified certain vulnerabilities in general controls involving (1) access to data and programs, (2) physical access, (3) contingency planning, and (4) security management.

We also identified vulnerabilities in the controls for two key BPD financial applications maintained and operated at the BPD data center in Parkersburg, West Virginia. Addressing these vulnerabilities requires (1) strengthening access controls by further restricting system access rights and improving security monitoring and (2) managing accuracy controls more effectively by ensuring that established procedures are followed to prevent unauthorized deletion of exception reports.

In most cases, BPD has corrected or is correcting the vulnerabilities that we identified. The following discussion provides a general summary of the vulnerabilities that existed on September 30, 1997. Those that we verified had been fully resolved subsequent to September 30, 1997, we have so noted. We will review the status of BPD's other corrective actions as part of our fiscal year 1998 financial audits.

Background

The Department of the Treasury is authorized by the Congress to borrow money on the credit of the United States to fund operations of the federal government. The Bureau of the Public Debt is the organizational entity

[1]Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of internal controls that, in the auditor's judgment, could adversely affect an entity's ability to (1) safeguard assets against loss from unauthorized acquisition, use, or disposition, (2) ensure the execution of transactions in accordance with management's authority and in accordance with laws and regulations, or (3) properly record, process, and summarize transactions to permit the preparation of the schedule or to maintain accountability for assets.

within Treasury that is responsible for prescribing the debt instruments and limiting and restricting the amount and composition of the debt. BPD accomplishes this by issuing marketable Treasury bills, notes, and bonds as well as nonmarketable securities, such as U.S. Savings Bonds. The bureau is also responsible for paying interest to investors and redeeming investors' securities. In addition, BPD has been given the responsibility to issue Treasury securities to trust funds for trust fund receipts not needed for current benefits and expenses.

During fiscal year 1997, BPD issued over $2.34 trillion in Treasury securities to the public while redeeming about $2.31 trillion of debt held by the public. Most of the $2.34 trillion was raised through more than 160 securities auctions as well as the continual sale of savings securities at 40,000 locations throughout the country and investments in securities by state and local governments. Further, there was $152 billion of net borrowings from federal entities, primarily trust funds.

BPD relies on a number of financial systems to process and track the money that is borrowed and to account for the securities it issues. One of its primary systems is the Public Debt Accounting and Reporting System, which is used to account for the federal debt. BPD also relies on various other systems to track marketable securities, savings bonds, and securities issued to state and local government entities and to generate interest transactions for the different securities. All of BPD's financial activities are processed at its data processing center in Parkersburg, West Virginia.

In carrying out its debt responsibilities, BPD receives assistance from Federal Reserve Banks (FRB) located throughout the country, which serve as Treasury's fiscal agents. For instance, FRBs issue Treasury securities in electronic (book entry) form upon authorization by the Treasury and administer principal and interest payments on these securities. There are 12 FRBs with 25 branches throughout the country.

FRBs use a number of information systems to help process issuance and redemption activities; generate interest payments; and account for marketable Treasury securities, nonmarketable savings securities, and savings securities stock. Data are initially processed at FRBs and then forwarded to BPD's Parkersburg, West Virginia, data center for further processing.

The overall effectiveness of the BPD computer controls depends on the controls implemented by BPD's Assistant Commissioner for the Office of

Information Technology. This person serves as Chief Information Officer and is responsible for overseeing the development, implementation, and operation of information processing systems.

Objectives, Scope, and Methodology

Our objectives were to evaluate and test the effectiveness of the controls over key financial management systems maintained and operated by BPD. Specifically, we evaluated general controls intended to

- protect data, files, and programs from unauthorized access, modification, and destruction;
- prevent the introduction of unauthorized changes to systems and applications software;
- ensure that system software development and maintenance, applications software development and maintenance, computer operations, security, and quality assurance are performed by different people;
- ensure recovery of computer processing operations in case of a disaster or other unexpected interruption; and
- ensure that an adequate computer security planning and management program is in place.

To evaluate the general controls, we identified and reviewed BPD's information system general control policies and procedures, conducted tests and observations of controls in operation, and held discussions with officials at the BPD data center to determine whether general controls were in place, adequately designed, and operating effectively. In addition, we attempted to obtain access to sensitive data and programs. These attempts, referred to as penetration testing, were performed with the knowledge and cooperation of BPD officials.

To evaluate certain application controls, we tested two key BPD financial applications maintained and operated at the data center. Specifically, we evaluated application controls intended to ensure that

- access privileges establish individual accountability and proper segregation of duties, limit the processing privileges of individuals, and prevent and detect inappropriate or unauthorized activities;
- data are authorized, converted to an automated form, and entered into the application accurately, completely, and promptly;
- data are properly processed by the computer and files are updated correctly; and

- files and reports generated by the application (1) represent transactions that actually occur and (2) accurately reflect the results of processing, and reports are controlled and distributed to the authorized users.

To assist in our evaluation and testing of general and application controls, we contracted with an independent public accounting firm. We determined the scope of our contractor's audit work, monitored its progress, and reviewed related working papers to ensure that the resulting findings were adequately supported.

During the course of our work, we communicated interim findings and recommended corrective actions to BPD officials who informed us of the steps they planned to take or had taken to address the vulnerabilities we identified. We performed follow-up work to assess the status of any corrective actions taken as of September 30, 1997. The results of the follow-up work were also communicated to BPD.

We performed our work at the BPD data center in Parkersburg, West Virginia, from March 1997 through January 1998 in accordance with generally accepted government auditing standards. We requested oral comments on a draft of this report from the Secretary of the Treasury or his designee. On August 31, 1998, the Commissioner of the Bureau of the Public Debt provided us with oral comments, which are discussed in the "Agency Comments" section.

Areas for Improvement in General Computer Controls

Our review of general controls over BPD's financial systems did not identify any weaknesses that placed BPD's financial information at significant risk of being accessed, compromised, or destroyed. However, we found certain vulnerabilities that warrant management's attention and action. Specifically, we found that BPD could improve its general controls by (1) strengthening logical access controls over the use of powerful system capabilities that can be used to access data and programs, (2) strengthening physical controls to further restrict and prevent unauthorized access, and (3) enhancing its service continuity and contingency plans. BPD could also improve its oversight and monitoring of computer security by ensuring that known security violations are investigated and resolved.

Access to Data and Programs

A key control used by organizations to protect and control access to information maintained in their systems is the use of logical access

controls. Logical access controls consist of safeguards, such as passwords, user IDs, and security software programs, that prevent unauthorized users from gaining access to computing resources and restrict the access of legitimate users to the specific systems, programs, and files that they need to conduct their work.

BPD did not adequately control powerful system capabilities to prevent unauthorized changes to data and programs that could adversely affect the integrity and availability of the on-line systems environment. We also identified vulnerabilities in certain controls that detect unauthorized access to BPD's systems.

Physical Access

Another key control for safeguarding financial data and computer resources from internal and external threats is physical access controls, such as locks, guards, fences, and surveillance equipment. Our review at the data center found physical access control vulnerabilities could allow access to sensitive areas within the BPD data center by employees whose jobs did not warrant such access.

Contingency Planning

An organization's ability to respond to and maintain service after an emergency can be significantly affected by how well it has planned for such contingencies and tested those plans. An organizational contingency plan describes how an organization will deal with a full range of emergencies, from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. The plan specifies the organization's emergency response, backup operations, and postdisaster recovery procedures to ensure the availability of critical resources and facilitate the continuity of operations. It also identifies essential business functions and prioritizes resources in order of criticality. To be most effective, a contingency plan should be periodically tested, and employees should be trained in and familiar with its use.

In reviewing BPD's service continuity and contingency planning, we found vulnerabilities related to the close proximity of off-site storage, currentness and completeness of contingency plan testing, and adequacy of the backup power supply.

Security Management

In addition to establishing controls and preparing emergency response plans, an effective computer security management program requires that

the organization be actively involved in planning and overseeing computer security activities. Such management involvement should include assigning explicit security responsibilities, regularly assessing risks, establishing and communicating security policies and procedures based on risks, and monitoring and periodically reviewing security controls.

In reviewing general controls, we found security management vulnerabilities related to (1) "conflict of interest" issues in the reporting and follow-up of security violations and (2) verifying that background checks have been performed before granting employees access to systems.

We also noted additional security management vulnerabilities related to the development of BPD-specific security policies and oversight of the security violation follow-up process. However, we verified that corrective actions resolving these vulnerabilities had been completed by BPD subsequent to September 30, 1997.

Application Controls Can Be Strengthened

In addition to testing general controls, we tested application controls for two key BPD financial applications maintained and operated at the BPD data center. We identified the following areas where improvements could be made: (1) strengthening access controls by further restricting system access rights and improving security monitoring and (2) managing accuracy controls more effectively by ensuring that established procedures are followed to prevent the unauthorized deletion of exception reports.

Access Controls

Like general access controls, access controls for specific applications should be established to ensure individual accountability and proper segregation of duties, limit the processing privileges of individuals, and prevent and detect inappropriate or unauthorized activities. For the applications reviewed, we found that BPD granted greater access rights to users than required for their jobs, maintained inadequate documentation of access authorizations granted to users, and did not adequately monitor user activities relating to the applications.

Accuracy Controls

Accuracy controls are one of the processing controls used to ensure that data are valid and correctly processed. For one application, we determined that the automated controls for identifying and correcting exceptions need improvement. Specifically, established procedures were

not followed to prevent inappropriate use of a powerful software utility to delete exception reports from production databases. The deletion of exception conditions may cause inaccuracies in the application's reporting.

FRBs' Computer Controls Can Be Improved

Because FRBs are integral to the operations of BPD, we also assessed general controls over BPD financial systems operated at FRBs and application controls for four key BPD financial applications maintained and operated by FRBs. Overall, we found these controls were effective. However, we found several vulnerabilities in general and application controls that require FRB management's attention and action. These include vulnerabilities in general controls involving (1) access to systems, programs, and data, including unauthorized external access and (2) service continuity and contingency planning. We also found vulnerabilities in access controls over two of the applications. During our review, we communicated our interim findings and recommended corrective actions for each specific finding to FRB management, and, in most cases, FRBs have acted or are acting to resolve the vulnerabilities that we identified. We will review the status of FRBs' other corrective actions as part of our fiscal year 1998 financial audits. Further, we are providing a separate report to the Board of Governors of the Federal Reserve System that summarizes the details of the control vulnerabilities at FRBs.

Other Controls

BPD implemented other controls that reduce the risk that the computer control vulnerabilities identified in this report could result in material losses or misstatements in the financial statements occurring and not being detected promptly. For instance, we determined that the assignment of duties for issuing and redeeming securities provides adequate segregation between FRB and BPD personnel, and that reconciliations of their independent records are performed daily. In addition, although the organizational placement of the security branch function could create "conflict of interest" situations, we found that discussion of security issues at periodic Executive Board meetings provides an opportunity for management to identify any potential instances of conflicts of interest.

Conclusions

Overall, the BPD and FRB general and application controls, combined with other effective features of their control environment, such as the clear separation of duties for issuing and redeeming securities, resulted in our opinion that management of BPD fairly stated that its related internal

controls, including computer controls, were effective. As evidenced by our work on the financial audit of the Bureau of the Public Debt's Fiscal Year 1997 Schedule of Federal Debt, we determined that the financial information presented on the schedule was materially correct. In addition, these controls have reduced BPD's susceptibility to inadvertent or deliberate misuse, fraudulent use, alteration, or destruction of financial data by users and others gaining access to the systems. However, left uncorrected, the vulnerabilities included in this report could increase the risk of inappropriate disclosure and modification of sensitive information, misuse or damage of computer resources, and disruption of critical operations and thus warrant management's attention and action.

Recommendations

To improve areas of vulnerability in general controls and application controls over BPD's financial systems cited in our July 31, 1998, "Limited Official Use" version of this report, we recommended in that report that you direct the Commissioner of the Bureau of the Public Debt to take the following actions.

- Correct each individual vulnerability we identified and communicated to BPD during our testing and summarized in the "Limited Official Use" report. Assign responsibility and accountability for correcting each vulnerability to designated individuals. These individuals should report regularly to the Commissioner on the status of all vulnerabilities, including actions taken to correct them.
- Work with FRBs to implement corrective actions to improve the computer control vulnerabilities related to BPD systems supported by FRBs that we identified and communicated to FRBs during our testing.

Agency Comments

BPD agreed with our findings and recommendations. The Commissioner of the Bureau of the Public Debt indicated that he was pleased that the review of BPD's general controls over financial systems did not identify any reportable conditions.[2] Further, he stated that in most cases, BPD has corrected or is already taking actions to resolve the vulnerabilities identified in this report.

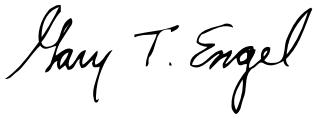
We are sending copies of this report to the Commissioner of the Bureau of the Public Debt; the Director of the Office of Management and Budget; the Chairmen and Ranking Minority Members of the Senate Committee on

[2]See footnote 1 for the definition of reportable conditions.

Appropriations and its Subcommittee on Treasury, General Government, and Civil Service, Senate Committee on Finance, Senate Committee on Governmental Affairs, Senate Committee on the Budget, House Committee on Appropriations and its Subcommittee on Treasury, Postal Service, and General Government, House Committee on Ways and Means, House Committee on Government Reform and Oversight and its Subcommittee on Government Management, Information and Technology, House Committee on the Budget; and other interested congressional committees. Copies will be made available to others upon request.

Should you or members of your staff have any questions concerning this report, please contact me at (202) 512-3406. Major contributors to this report are listed in appendix I.

Sincerely yours,



Gary T. Engel
Associate Director
Governmentwide Accounting and
Financial Management Issues

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.

J. Lawrence Malenich, Assistant Director
Barbara S. Oliver, Audit Manager
Gregory C. Wilshusen, Assistant Director—Technical Advisor

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 37050
Washington, DC 20013

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 (202) 512-6061, or TDD (202) 512-2537.

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

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