United States General Accounting Office

GAO

Report to the Secretary of the Treasury

August 2000

# BUREAU OF THE PUBLIC DEBT

# Areas for Improvement in Computer Controls



GAO/AIMD-00-269

GAO
Accountability * Integrity * Reliability

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

**Accounting and Information**
**Management Division**

B-285216

August 9, 2000

The Honorable Lawrence H. Summers
The Secretary of the Treasury

Dear Mr. Secretary:

In connection with fulfilling our requirement to audit the U.S. government's fiscal year 1999 financial statements,[1] we audited and reported on the Bureau of the Public Debt's (BPD) Schedules of Federal Debt managed by BPD for the fiscal years ended September 30, 1999 and 1998.[2] Our review of the general and application computer controls over key BPD financial systems was performed as part of these audits. On June 27, 2000, we issued a Limited Official Use report to you detailing the results of our review. This excerpted version of the report for public release summarizes (1) the vulnerabilities we identified and recommendations we made and (2) our follow-up on previously reported vulnerabilities.

This report presents the results of our tests of the effectiveness of general and application controls that support key automated financial systems and our follow-up on the status of BPD's corrective actions to address vulnerabilities identified in our fiscal years 1998 and 1997 audits.[3] These systems, some of which are operated and maintained by the Federal Reserve Banks (FRB), process investments in and redemption of Treasury securities, generate interest payments, account for the resulting federal debt, and provide financial reports to the public and the federal government. We also assessed the general and application controls over key BPD systems that the FRBs maintain and operate and have issued a separate report to the Board of Governors of the Federal Reserve on the results of our testing.[4]

---

[1] 31 U.S.C. 331 (e) (1994).

[2] *Financial Audit: Bureau of the Public Debt's Fiscal Years 1999 and 1998 Schedules of Federal Debt* (GAO/AIMD-00-79, March 1, 2000).

[3] *Bureau of the Public Debt: Areas for Improvement in Computer Controls* (GAO/AIMD-99-207, July 16, 1999).

[4] *Federal Reserve Banks: Areas for Improvement in Computer Controls* (GAO/AIMD-00-218, July 7, 2000).

As we reported in connection with our audit of the Schedules of Federal Debt, BPD's internal control over financial reporting and compliance, including computer controls, was effective. In that report, we did not identify any reportable conditions.[5] However, we identified vulnerabilities involving general and application computer controls that we did not consider reportable conditions, but, if left uncorrected, increase the risk of inappropriate disclosure or modification of sensitive information or disruption of critical operations. These vulnerabilities warrant BPD management's attention and action. In light of the significant reliance on interconnected automated systems between BPD and the FRBs to support program operations and to replace manual procedures and paper documents, well-designed and properly implemented general and application controls are essential to protecting BPD's computer resources and ensuring continuity of operations. While performing our work, we communicated detailed information regarding our findings to BPD management. This report provides an overall assessment and summary of BPD's computer control vulnerabilities and recommendations we made.

## Results in Brief

Overall, we found that BPD's general and application controls combined with other management and manual reconciliation controls were effective in ensuring BPD's ability to report reliable financial information and data. Although various management and reconciliation controls help BPD detect potential irregularities or improprieties in its financial data or transactions, these types of compensating controls do not prevent certain threats to its computer resources or operating environment from unintentional errors or omissions, or intentional modification, disclosure, or destruction of data and programs by disgruntled employees, intruders, or hackers. Thus, the vulnerabilities we noted increase the risks of inappropriate disclosure and modification of sensitive data and programs, misuse or damage of computer resources, or disruption of critical operations. BPD informed us that it agreed with our findings and that in most cases, it had subsequently corrected or was in the process of correcting vulnerabilities that we identified.

[5]Reportable 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 that could adversely affect the organization's ability to meet the objective of reliable financial reporting and compliance with applicable laws and regulations.

Our fiscal year 1999 audit procedures identified certain general control vulnerabilities in BPD's entitywide security management program, access controls, application software development and change controls, and service continuity. We also identified vulnerabilities in the application controls over four key BPD financial applications maintained and operated at the BPD data center. Specifically, we identified vulnerabilities in the authorization controls over two of the four key BPD financial applications we reviewed. In addition, we identified completeness and accuracy control vulnerabilities over a third key BPD financial application and authorization and accuracy control vulnerabilities over a fourth key BPD financial application. Our follow-up on the status of BPD's corrective actions to address vulnerabilities identified in our fiscal years 1998 and 1997 audits found that BPD had corrected or mitigated the risks associated with 5 of the 17 general and application control vulnerabilities discussed in our prior reports. Additionally, BPD is in the process of addressing the remaining 12 general and application control vulnerabilities discussed in our prior years' reports.

## Background

The Department of the Treasury is authorized by Congress to borrow money on the credit of the United States to fund operations of the federal government. Within Treasury, BPD is responsible for prescribing the debt instruments, limiting and restricting the amount and composition of the debt, paying interest to investors, and accounting for the resulting debt. In addition, BPD has been given the responsibility for issuing Treasury securities to trust funds for trust fund receipts not needed for current benefits and expenses.

As of September 30, 1999 and 1998, federal debt managed by BPD totaled about $5.6 trillion and $5.5 trillion, respectively, for moneys borrowed to fund the government's operations. These balances consisted of approximately (1) $3.6 trillion as of September 30, 1999, and $3.8 trillion as of September 30, 1998, owed to the public, and (2) $2.0 trillion as of September 30, 1999, and $1.7 trillion as of September 30, 1998, owed to federal entities, such as the Social Security trust funds. Total interest expense for fiscal years 1999 and 1998 was $356 billion and $363 billion, respectively.

BPD relies on a number of interconnected financial systems and electronic data to process and track the money that is borrowed and to account for the securities it issues. FRBs also provide fiscal agent services on behalf of BPD, which primarily consist of issuance, servicing, and redemption of

Treasury securities; processing secondary market transactions; and handling the related transfers of funds. The FRBs use a number of financial systems to process debt-related transactions throughout the country. Detailed data initially processed at FRBs are summarized and then forwarded electronically to BPD's data center for matching, verification, and posting to the general ledger.

## 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 and to determine the status of the computer control vulnerabilities identified in our fiscal years 1998 and 1997 audits. We used a risk-based and a rotation approach for testing general and application controls. Under that methodology, every 3 years the data center and each key application is subject to a full scope review that includes testing in all of the computer control areas defined in our *Federal Information System Controls Audit Manual* (FISCAM).[6]

The scope of our work for fiscal year 1999 included follow-up on vulnerabilities identified in our prior years' reports and FISCAM testing that was limited to five general control areas, which are

- entitywide security management program,
- access controls,
- segregation of duties,
- system software, and
- service continuity.

To evaluate these general controls, we identified and reviewed BPD's information system general control policies and procedures; observed controls in operation; conducted tests of controls, which in some instances included selecting items using a method where the results are not projectable to the population; and held discussions with officials at the BPD data center to determine whether controls were in place, adequately designed, and operating effectively. Additionally, through our external and internal network security penetration testing, we attempted to access sensitive data and programs through "brute-force attack programs." These

[6]GAO/AIMD-12.19.6, January 1999.

attempts were performed with the knowledge and cooperation of certain BPD officials.

We also used a rotation approach to evaluate controls over selected key applications. We performed a full-scope application controls review of one key financial application to determine whether the application is designed 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;
- erroneous data are captured, reported, investigated, and corrected; and
- files and reports generated by the application represent transactions that actually occur and accurately reflect the results of processing, and reports are controlled and distributed only to authorized users.

The scope of our work over three other key financial applications was limited to follow-up on vulnerabilities that we identified in our fiscal years 1998 and 1997 audits.

To evaluate application controls in both the full-scope and the follow-up reviews, we identified and reviewed application control policies and procedures; observed controls in operation; conducted tests of controls, which in some instances included selecting items using a method where the results are not projectable to the population; and held discussions with officials to determine whether controls were in place, adequately designed, and operating effectively.

Because FRBs are integral to the operations of BPD, we assessed the general controls over BPD systems that FRBs maintain and operate. We also evaluated application controls over two key BPD financial applications maintained and operated by the FRBs. We followed up on the status of FRB's corrective actions to address vulnerabilities identified in our fiscal years 1998 and 1997 audits.[7]

[7] *Federal Reserve Banks: Areas for Improvements in Computer Controls* (GAO/AIMD-99-245, August 16, 1999).

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

During the course of our work, we communicated our findings to BPD management who informed us that BPD has taken or plans to take corrective actions to address the vulnerabilities identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 2000 financial statements.

We performed our work at the BPD data center from September 1999 through February 2000. Our work was performed in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from the Department of Treasury. Its comments are discussed in the "Agency Comments" section of this report.

## Areas for Improvement in BPD's General Computer Controls

General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. General controls establish the environment in which application systems and controls operate. They include an entitywide security management program, access controls, system software controls, application software development and change controls, segregation of duties, and service continuity controls. An effective general control environment would (1) ensure that an adequate computer security management program is in place, (2) protect data, files, and programs from unauthorized access, modification, disclosure, and destruction, (3) limit and monitor access to programs and files that control computer hardware and secure applications, (4) prevent unauthorized programs or unauthorized changes to an existing program from being implemented, (5) prevent any one individual from controlling key aspects of computer-related operations, and (6) ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption.

We identified vulnerabilities in the entitywide security management program, access controls, application software development and change controls, and service continuity. These vulnerabilities, if left uncorrected, increase the risk of inappropriate disclosure or modification of sensitive data and programs or disruption of critical operations.

## Entitywide Security Management Program

An entitywide security management program is the foundation of an entity's security control structure and should establish a framework for continual (1) risk assessments, (2) development and implementation of effective security procedures, and (3) monitoring and evaluation of the effectiveness of security procedures. A well-designed entitywide security management program helps to ensure that security controls are adequate, properly implemented, and applied consistently across the entity, and that responsibilities for security are clearly communicated and understood.

As part of its entitywide security management program, BPD requires all data center personnel to undergo extensive background investigations prior to being employed. All employees granted a clearance are also required to undergo extensive clearance investigations prior to being granted a clearance. In addition, all employees are subject to background reinvestigations every 5 years. During our testing, we found that 11 of 23 employees holding Secret through Top Secret clearances did not have the required Classified Information Non-Disclosure Agreement (Standard Form 312) in their personnel files. Standard Form 312 is intended to be an agreement between the signatory and the U.S. government legally binding the signatory to never divulge classified information to anyone unless certain conditions allowing for the divulgence of the information have been met.[8]

Without a Standard Form 312 in each employee's personnel file, BPD cannot provide evidence that the employee attended required security briefings. Therefore, the potential exists that BPD employees with a security clearance may not know the roles and responsibilities to which they are legally bound once granted a security clearance.

## Access Controls

Access controls are designed to limit or detect access to computer programs, data, equipment, and facilities to protect these resources from unauthorized modification, disclosure, loss, or impairment. Such controls include logical and physical security controls.

Logical security control measures involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to

[8]Subsequent to September 30, 1999, BPD officials informed us that BPD had corrected this vulnerability. We plan to verify the corrective actions reportedly taken by BPD during our audit of the U.S. government's fiscal year 2000 financial statements.

input unique user identifications (ID), passwords, or other identifiers that are linked to predetermined access privileges. Logical security controls restrict the access of legitimate users to the specific systems, programs, and files they need to conduct their work and prevent unauthorized users from gaining access to computer resources.

As reported in the prior year, we found internal network access control vulnerabilities that expose BPD systems to the risk of unauthorized access to systems, sensitive data, and computing resources. While a disgruntled employee could disrupt BPD's operations or obtain unauthorized access to other system resources, the segregation of responsibilities between BPD and the FRBs and the transmission of only summary-level information from the FRBs to BPD adequately prevents one individual from completing a debt-related transaction. In addition, other key management and manual reconciliation controls at BPD help to detect erroneous or fraudulent financial data or transactions. These include (1) extensive background investigations on all employees, (2) management monitoring and review of assigned workloads, exception reports, and unauthorized transactions exception reports, and (3) daily independent manual and automated reconciliations of Treasury debt security issuance, redemption, and interest payment transactions with the applicable FRBs and Treasury's Financial Management Service. Due to the sensitive nature of the internal network control vulnerabilities we identified, these issues are described in the separate Limited Official Use report issued to you on June 27, 2000.

Another important aspect of access controls includes physical security controls such as locks, guards, badges, alarms, and similar measures (used alone or in combination) that help to safeguard computer facilities and resources from intentional or unintentional loss or impairment by limiting access to the buildings and rooms where they are housed.

During our fiscal year 1999 audit, we found that the mainframe consoles were located in the same operational work area as the Help Desk function, making them susceptible to being physically compromised. Without physically separating the Help Desk area from these consoles, Help Desk operators could potentially access the mainframe consoles and intentionally or unintentionally process commands that could alter or interrupt computer operations.

We also identified vulnerabilities in physical security controls over access to the command center and the printer room. Specifically, (1) some data center users who have been granted access to the computer room may

potentially have inappropriate access to the printer room, (2) employees with access to the computer room through certain hallway doors also have unrestricted access to the command center and the printer room, and (3) employees granted access to the command center may have unauthorized access to the printer room. These conditions existed because the doors connecting the computer room, the printer area, and the command center did not have card-key reader locks or other mechanisms to restrict the entry and exit of personnel. Without proper physical safeguards to prevent unauthorized access, accidental or intentional destruction, capture, or disclosure of proprietary and confidential information could result. While this condition existed at September 30, 1999, BPD subsequently resolved this issue in December 1999 by installing card-key readers at the exit points for all of the aforementioned doors.

## Application Software Development and Change Controls

Controls over the design, development, and modification of application software help to ensure that all programs and program modifications are properly authorized, tested, and approved. Such controls also help prevent security features from being inadvertently or deliberately turned off and processing irregularities or malicious code from being introduced.

As we reported in our fiscal year 1998 audit, we found that various BPD user groups and their supporting application developers did not consistently follow Treasury's internal guidelines regarding the application software development and change process. Specifically, customer technical representative groups, who handle enhancements, maintenance requests, and emergency change requests, followed different procedures and different standards of documentation for processing these enhancements and requests. Contributing factors to these conditions were the use of several different change and problem management tools and the lack of standard practices requiring (1) written authorization to move application software from the acceptance region to the production region and (2) retention guidelines for user acceptance test plans and results. During our fiscal year 1999 review of this process for the five key applications at BPD, we found the following.

- Our prior year recommendation to use a single central change and problem management tool for managing software changes, including user change requests, and reporting of software problems, had not been fully implemented.[9]
- Our prior year recommendation to update BPD's Application Systems Division handbook, consisting of requiring formal approvals of program changes and retaining user acceptance and test plans and results, had not been made.

During our fiscal year 1999 testing, we found that BPD was unable to consistently provide evidence of formal written approval on the acceptance test results for system software changes. In the absence of formal written approvals on the acceptance test results, system and application software changes could be migrated to the production environment without proper testing and authorization, thereby increasing the risk of disrupting operations or causing other unexpected operating results. Specifically, we found that 37 of the 45 system software changes we tested were not approved via the automated approval feature of the problem and change management system. BPD only required verbal approvals, which BPD officials stated were obtained during weekly change control meetings prior to introducing changes into the production environment. Consequently, effective evidence of final approvals on the acceptance test results is unavailable to BPD management and other dependent parties, such as those affected by a change.

To a certain extent, BPD's low turnover and extensive in-house knowledge reduce the risk that knowledge of the applications could be lost or application maintenance could become inefficient. However, these do not replace the benefits of a well-designed and managed application software development and change control process to prevent unintentional or intentional programming errors or omissions.

## Service Continuity

An organization's ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information that is maintained electronically. For this reason, organizations should have (1) established procedures for protecting information resources and

[9]To achieve consistency and continuity of operations in the current change control environment, BPD moved the last of its five key application systems under a single control mechanism in November 1999.

minimizing the risk of unplanned interruptions and (2) plans for recovering critical operations should interruptions occur. A contingency or disaster recovery plan specifies emergency response, backup operations, and postdisaster recovery procedures to ensure the availability of critical resources and facilitate the continuity of operations in an emergency. It addresses how an organization will deal with a range of contingencies, from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. The plan also identifies essential business functions and ranks resources in order of criticality. To be most effective, a contingency plan should be periodically tested in disaster simulation exercises, and employees should be trained in and familiar with its use.

In reviewing BPD's service continuity and contingency planning, we found that while progress was being made, corrective actions had not been completed for the vulnerabilities we identified in our prior year audits related to (1) contingency plan testing and (2) the adequacy of the backup power supply.

The limited contingency plan testing conducted to date provides some level of assurance for certain components of BPD's disaster recovery plan. However, events, such as changes to BPD's computing environment (including hardware, software, networks, procedures, and personnel), increase the risk that BPD may not be prepared to effectively prioritize recovery activities, integrate recovery steps effectively, or fully recover systems during an emergency. BPD is planning a full system disaster recovery test in fiscal year 2000.

## BPD's Application Controls Can Be Strengthened

Application 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.

In addition to testing general controls, we tested application controls for four key financial applications and identified vulnerabilities in authorization, completeness, and accuracy controls.

### Authorization Controls

Authorization controls for specific applications, similar to general access controls, 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.

During our review of the application controls for one key financial application, we found the following vulnerabilities involving inappropriate access, which could provide an employee with unauthorized access rights to compromise data integrity and confidentiality.

- During our review of functional group access, we found that employees in one group had inappropriate transaction processing capabilities for their job functions. While this condition existed at September 30, 1999, BPD resolved this issue in October 1999.
- Four employees with different job functions in one group and another employee from a second group had inappropriate access to the application. Specifically, we selected 27 critical or sensitive transaction codes representing the greatest risk to the application (consisting primarily of update, add, cancel, and verify capabilities) for testing and found that four employees in one group had inappropriate access to the on-line processing screens for 20 of the 27 critical or sensitive transaction codes selected. In addition, one employee in a second group had inappropriate access to the on-line processing screens for 17 of the 27 critical or sensitive transaction codes selected. Inappropriate access to the on-line transaction processing capabilities could result in the unintentional or intentional alteration, modification, or disclosure of sensitive or proprietary data.
- User group identification maintenance needs improvement in the application. We found user group identifications with mislabeled titles, user groups with no members, and groups that had been combined. In addition, we found that one group does not have position description documentation for each position. Lack of position descriptions, inappropriate group names, groups without users assigned, combined groups, and outdated group names may lead to improper classification of a user. As such, an employee could obtain inappropriate access rights to compromise data integrity and confidentiality.

In addition, as we previously reported in our fiscal year 1998 audit, we found that policies and procedures for performing changes to master data in another key financial application have not been formally documented in writing, increasing the risk that unauthorized changes could be made. In response to our prior years' recommendation, BPD developed a formal

change control procedure, which was instituted in January 1999. In order to verify that BPD personnel were adhering to these documented policies and procedures, we selected 45 changes that were implemented during fiscal year 1999. We found that BPD was not fully adhering to its policies and procedures as three changes were missing signatures that would designate final approval of the change.

Also, as we previously reported in our fiscal years 1998 and 1997 audits, our fiscal year 1999 testing of authorization controls for a third key financial application found that access to this application was not consistently established in accordance with management's authorization. In addition, policies and procedures did not clearly define the responsibilities for security monitoring for this application.

## Completeness Controls

Completeness controls are designed to help ensure that all transactions are processed and missing transactions are identified. Common completeness controls include the use of header and trailer records with record counts and control totals, computer sequence checking, computer matching of transaction data with data in a master or suspense file, and checking of reports for transaction data. Without such automated controls, there is an increased risk that incomplete financial information or transactions could be transmitted and not promptly detected resulting in a misstatement in financial or other data.

As we previously reported in our fiscal year 1998 audit, we found that certain interface files developed by BPD for one of the key applications did not contain trailer records with record counts or control totals because it is not a requirement of BPD's software design policy. In addition, certain of these interface files did not contain header records. Our fiscal year 1999 audit found that this issue had not been resolved. BPD continues to rely on manual detection and monthly reconciliation controls to help ensure that files are successfully received and transactions are processed and reported. However, these manual controls do not replace the efficiencies gained by using automated control procedures that are performed on a real-time basis to identify and prevent the transmission of incomplete, erroneous, or fraudulent data. BPD management stated that due to Y2K concerns, this issue would be addressed during fiscal year 2000.

## Accuracy Controls

The recording of valid and accurate data into application systems is essential to an effective system that produces reliable results. Accuracy

controls include (1) well-designed data entry procedures, (2) data validation and editing to identify erroneous data, (3) reporting, investigating, and correcting erroneous data, and (4) review and reconciliation of output.

As we previously reported in our fiscal year 1998 audit, we found that a program designed to automatically clear exception reports from one of BPD's key applications does not operate properly. Instead, BPD continues to use a powerful software utility, on which we reported in our fiscal year 1997 audit, to delete exception reports from the production databases. During our fiscal year 1999 audit, we found that BPD continues to use the powerful software utility to delete exception reports because system enhancements have not been fully completed and implemented. Although BPD has developed informal procedures for using the powerful software utility, the privileges provided by the utility go far beyond those needed by an individual to clear exception reports. Consequently, there is the risk that an individual could use the more powerful features of the software utility to unintentionally or intentionally delete critical production data or disrupt operations.

According to BPD, during fiscal year 1998, the introduction of a new application improved the processing cycle times for recording savings bond transactions in one key application from 6 weeks to 3 days. This new application allowed BPD to report transfer matching errors more promptly. However, BPD had not revised its procedures by increasing the frequency of its exception report review to respond to the significant reduction in processing cycle times. Consequently, matching errors will not be corrected promptly. In response to our prior year's recommendation, BPD updated its review procedures to require daily review of the exception reports, notification to the responsible reporting entity by close of business the same day, and correction of the transfer matching error within 2 days. However, during our fiscal year 1999 audit, we selected 45 exception reports for review and found that transfer matching errors were often outstanding for more than a week.

## FRB Computer Controls Can Be Improved

Because FRBs are integral to the operations of BPD, we assessed the effectiveness of general and application controls that support key BPD financial systems maintained and operated by the FRBs. During our follow-up work, we found that the FRBs had corrected many of the vulnerabilities relating to BPD systems that were identified in our prior years' reports and that work is in progress to address the remaining vulnerabilities. Our fiscal

year 1999 audit procedures identified vulnerabilities in general controls that do not have a significant adverse impact on BPD financial systems, but nonetheless warrant FRB management's attention and action. These include vulnerabilities in (1) the entitywide security management program, (2) controls over access to data, programs, and computing resources, (3) application software development and change controls, (4) system software controls, and (5) segregation of duties. We also found vulnerabilities in authorization controls over one key application. We provided details of these matters in a separate report to the Board of Governors of the Federal Reserve System along with our recommendations for improvement. FRB management has informed us that the FRBs have taken or plan to take corrective actions to address the vulnerabilities we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 2000 financial statements.

## Conclusion

Well-designed and properly implemented general and application controls are essential to protecting BPD's computer resources and operational environment from the risks of inappropriate disclosure and modification of sensitive information, misuse or damage of computer resources, and disruption of critical operations. BPD needs to take preventive measures to further reduce its exposure to certain threats to its computer resources and operating environment due to unintentional errors or omissions, or intentional modification, disclosure, or destruction of data and programs by disgruntled employees, intruders, or hackers. As we noted, BPD is in the process of addressing most of the vulnerabilities we identified as part of our fiscal years 1998 and 1997 audits. BPD has already taken some actions to resolve the new vulnerabilities we identified during our fiscal year 1999 audit, but further actions are required to fully address the vulnerabilities discussed in this report.

## Recommendations

In our June 27, 2000, Limited Official Use version of this report, we recommended that the Secretary of the Treasury direct the Commissioner of the Bureau of the Public Debt to take specific actions to correct each of the individual vulnerabilities that were identified during our testing and summarized in that report.

We also recommended that the Secretary of the Treasury direct the Commissioner of BPD to work with the FRBs to implement corrective actions to resolve the computer control vulnerabilities related to BPD

systems supported by FRBs that we identified and communicated to the FRBs during our testing.

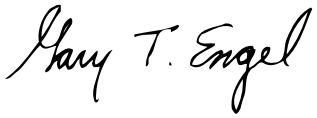
## Agency Comments

In commenting on a draft of this report, BPD agreed with our findings. The Commissioner of the Bureau of the Public Debt stated that in most cases, BPD had subsequently corrected or is already taking actions to resolve the vulnerabilities identified in the report.

We are sending copies of this report to Senator Robert C. Byrd, Senator Ben Nighthorse Campbell, Senator Pete V. Domenici, Senator Byron L. Dorgan, Senator Frank R. Lautenberg, Senator Joseph Lieberman, Senator Daniel Patrick Moynihan, Senator William V. Roth, Jr., Senator Ted Stevens, and Senator Fred Thompson and to Representative Bill Archer, Representative Spencer Bachus, Representative Dan Burton, Representative Stephen Horn, Representative Steny H. Hoyer, Representative John R. Kasich, Representative Jim Kolbe, Representative David R. Obey, Representative Charles B. Rangel, Representative John M. Spratt, Jr., Representative Jim Turner, Representative Henry A. Waxman, and Representative C.W. Bill Young, in their capacities as Chairmen or Ranking Minority Members of Senate or House Committees and Subcommittees. We are also sending copies of this report to Mr. Van Zeck, Commissioner, Bureau of the Public Debt; the Honorable Jeffrey Rush, Jr., Inspector General, Department of the Treasury; the Honorable Jacob J. Lew, Director, Office of Management and Budget; and other agency officials. Copies will also be made available to others upon request.

If you have any questions regarding this report, please contact me at (202) 512-3406. Key contributors to this assignment were J. Lawrence Malenich, Paula M. Rascona, and Dawn B. Simpson.

Sincerely yours,



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

## Ordering Information

**The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. 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**

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

***Orders by phone:***
**(202) 512-6000**
**fax: (202) 512-6061**
**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.**

***Orders by Internet:***
**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**

## To Report Fraud, Waste, or Abuse in Federal Programs

***Contact one:***

- **Web site: http://www.gao.gov/fraudnet/fraudnet.htm**
- **e-mail: fraudnet@gao.gov**
- **1-800-424-5454 (automated answering system)**

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

**Official Business**
**Penalty for Private Use $300**

**Address Correction Requested**

**Bulk Rate**
**Postage & Fees Paid**
**GAO**
**Permit No. GI00**