GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 14, 2007

The Honorable Van Zeck
Commissioner, Bureau of the Public Debt

Subject: *Bureau of the Public Debt: Areas for Improvement in Information Security Controls*

Dear Mr. Zeck:

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, 2006 and 2005.[2] As part of these audits, we performed a review of the general and application information security controls over key BPD financial systems.

In our audit report on the Schedules of Federal Debt for the fiscal years ended September 30, 2006 and 2005, we concluded that 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, 2006, that provided reasonable assurance that misstatements, losses, or noncompliance material in relation to the Schedule of Federal Debt would be prevented or detected on a timely basis. We found matters involving information security controls that we do not consider to be reportable conditions[3] but that nevertheless warrant BPD management's attention and action. BPD mitigated the potential effect of such issues with physical security measures, a program of monitoring user and system activity, and compensating management and reconciliation controls.

This report presents the issues identified during our fiscal year 2006 testing of the general and application information security controls that support key BPD automated financial systems relevant to BPD's Schedule of Federal Debt. This report also includes the results of our follow-up on the status of BPD's corrective actions to

[1] 31 U.S.C. § 331(e).

[2] GAO, *Financial Audit: Bureau of the Public Debt's Fiscal Years 2006 and 2005 Schedules of Federal Debt*, GAO-07-127 (Washington, D.C.: Nov. 7, 2006).

[3] 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, which could adversely affect the organization's ability to meet the objectives of reliable financial reporting and compliance with applicable laws and regulations.

address recommendations that were contained in our prior years' audits and open as of September 30, 2005. In a separately issued Limited Official Use Only report, we communicated detailed information regarding our findings to BPD management. We also assessed the general and application information security controls over key BPD financial systems that the Federal Reserve Banks (FRB) maintain and operate on behalf of BPD. We have communicated the results of such testing to the Board of Governors of the Federal Reserve System.

Results in Brief

Our fiscal year 2006 audit procedures identified eight new information security control issues, of which seven relate to general controls and the other to an application control. Specifically, the general information security control issues were in the areas of entitywide security program planning and management, access control, application software development and change control, and system software. The application information security control issue relates to the reporting of unusual activity. In the Limited Official Use Only report, we made eight recommendations to address these issues.

During our follow-up on the status of BPD's corrective actions to address 11 open recommendations related to information security control issues identified in prior years' audits for which actions were not complete as of September 30, 2005, we found the following:

- As of September 30, 2006, corrective action on 8 of the 11 recommendations had been completed.

- Corrective action was in progress as of September 30, 2006, on the three remaining open recommendations, which relate to access controls.

BPD provided comments on the detailed findings and recommendations in the separately issued Limited Official Use Only report. In those comments, the Commissioner of the Bureau of Public Debt stated that of the 11 recommendations, which include 3 from a prior year, 4 have been completely resolved, and corrective actions for the remaining 7 are in progress. The Commissioner also stated that BPD intends to fully implement the remaining recommendations by May 2008.

Background

The Department of the Treasury (Treasury) is authorized by Congress to borrow money on the credit of the United States to fund federal operations. Treasury is responsible for prescribing the debt instruments and otherwise limiting and restricting the amount and composition of the debt. BPD, an organizational entity within the Fiscal Service of the Department of the Treasury, is responsible for issuing and redeeming debt instruments, 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, 2006 and 2005, federal debt managed by BPD totaled about $8.5 trillion and $7.9 trillion, respectively, for moneys borrowed to fund the government's operations. These balances consisted of approximately (1) $4.8 trillion and $4.6 trillion of debt held by the public as of September 30, 2006 and 2005, respectively; and (2) $3.7 trillion and $3.3 trillion of intragovernmental debt holdings as of September 30, 2006 and 2005, respectively. Total interest expense on federal debt managed by BPD for fiscal years 2006 and 2005 was about $404 billion and $355 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. Many of the FRBs provide fiscal agent services on behalf of BPD, which primarily consist of issuing, servicing, and redeeming Treasury securities held by the public and handling the related transfers of funds. The FRB uses a number of financial systems to process debt-related transactions throughout the country. Detailed data initially processed at the 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 the effectiveness of the general and application information security controls over key financial management systems maintained and operated by BPD relevant to the Schedule of Federal Debt and to determine the status of corrective actions taken in response to the recommendations in our prior years' reports for which actions were not complete as of September 30, 2005. We use a risk-based, rotation approach for testing general information security controls. Each general information security control area is subjected to a full-scope review, including testing, at least every 3 years. The general information security control areas we review are defined in the *Federal Information System Controls Audit Manual.*[4] Areas considered to be of higher risk are subject to more frequent review. Each key application is subjected to a full-scope review every year.

To evaluate general and application information security controls, we identified and reviewed BPD's information system general and application information security control policies and procedures, observed controls in operation, conducted tests of controls, and held discussions with officials at the BPD data center to determine whether controls were in place, adequately designed, and operating effectively.

The scope of our work for fiscal year 2006 as it relates to general information security controls included following up on open recommendations from our prior years' reports and conducting a full-scope review of the general controls which includes a review of the entitywide security program planning and management, access control, application software development and change control, system software, segregation of duties, and service continuity. In addition, we performed security diagnostics and

[4] GAO, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

vulnerability assessment testing of BPD's internal and external information system environment.

Full-scope application information security control reviews were performed on six key BPD applications to determine whether the applications are designed to ensure that

- access privileges (1) establish individual accountability and proper segregation of duties, (2) limit the processing privileges of individuals, and (3) 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 as it relates to application information security controls also included following up on open recommendations from our prior year's report for which actions were not complete as of September 30, 2005. We also reviewed the application information security control audit documentation from the work performed by the Treasury Office of Inspector General's contractor on another key BPD application.

Because the FRBs are integral to the operations of BPD, we assessed the general information security controls over financial systems that the FRBs maintain and operate relevant to the Schedule of Federal Debt. We also evaluated application information security controls over six key financial applications maintained and operated by the FRBs.

The evaluation and testing of information security controls, including the follow-up on the status of BPD corrective actions to address open recommendations in our fiscal year 2005 report, were performed by the independent public accounting (IPA) firm of Cotton and Company, LLP. We agreed on the scope of the audit work, monitored the IPA firm's progress, and reviewed the related audit documentation to ensure that the 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 action to address the control issues we identified. We plan to follow up on these matters during our audit of the fiscal year 2007 Schedule of Federal Debt.

We performed our work at the BPD data center from April 2006 through October 2006. Our work was performed in accordance with U.S. generally accepted government auditing standards. As noted earlier, we obtained agency comments on the detailed findings and recommendations in a draft of the separately issued Limited

Official Use Only report. BPD's comments are summarized in the Agency Comments and Our Evaluation section of this report.

Assessment of BPD's Information Security Controls

General information security controls are the structure, policies, and procedures that apply to an entity's overall computer operations. General information security controls establish the environment in which application systems and controls operate. They include entitywide security program planning and management, access control, system software, application software development and change control, segregation of duties, and service continuity. An effective general information security control environment helps (1) ensure that an adequate entitywide 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 the introduction of unauthorized changes to systems and applications software; (5) prevent any one individual from controlling key aspects of computer-related operations; and (6) ensure the recovery of computer processing operations in the event of a disaster or other unexpected interruption.

Our fiscal year 2006 testing identified opportunities to strengthen certain information security controls that support key BPD automated financial systems relevant to BPD's Schedule of Federal Debt. Specifically, our audit procedures identified eight new information security control issues, of which seven relate to general controls and the other to an application control. The general information security control issues included two issues related to the entitywide security program planning and management, three issues related to logical access control, one issue related to application software development and change control, and one issue related to system software. The application information security control issue related to audit logs.

An entitywide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

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 access controls and physical access controls. Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input unique user identifications (ID), passwords, or other identifiers that are linked to predetermined access privileges. Logical access 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.

Application software development and change controls help ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled. Without proper application software development and change controls, there is a risk that security features could be inadvertently or deliberately omitted or "turned off" or that processing irregularities or malicious code could be introduced.

System software coordinates and helps control the input, processing, output, and data storage associated with all of the applications that run on a system. System software includes operating system software, system utilities, file maintenance software, security software, data communications systems, and database management systems. Controls over access to and modifications of system software are essential to protect the overall integrity and reliability of information systems.

Application information security 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 information security controls help to ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.

In a separately issued Limited Official Use Only report, we communicated detailed information regarding our findings to BPD management and made eight recommendations.

During our follow-up on the status of BPD's corrective actions to address 11 open recommendations related to information security control issues identified in prior years' audits for which actions were not complete as of September 30, 2005, we found the following:

- As of September 30, 2006, corrective action on 8 of the 11 recommendations had been completed.

- Corrective action was in progress as of September 30, 2006, on the three remaining open recommendations which relate to access controls. As such, we are reaffirming our three previous recommendations.

None of our findings pose significant risks to the BPD financial systems. In forming our conclusions, we considered the mitigating effects of physical security measures, a program of monitoring user and system activity, and reconciliation controls that are designed to detect potential irregularities or improprieties in financial data or transactions. Nevertheless, these findings warrant management's attention and action to limit the risk of unauthorized access, disclosure, loss, or impairment; modification of sensitive data and programs; and disruption of critical operations.

Assessment of FRB Information Security Controls

Because the FRBs are integral to the operations of BPD, we assessed the general and application information security controls over key financial systems maintained and operated by the FRBs on behalf of BPD. Our fiscal year 2006 audit procedures did not identify any new information security control issues over such systems. We have communicated the results from that assessment to the Board of Governors of the Federal Reserve System.

Conclusion

BPD has made significant progress in addressing open recommendations from our prior years' audits and has informed us that corrective actions have been taken or are being taken to address the three remaining unresolved issues. We therefore reaffirm our three recommendations related to these open issues.

Our fiscal year 2006 audit identified eight new information security control issues, of which seven relate to general controls and the other to an application control. For these identified issues, we are making eight recommendations. BPD informed us that it has taken, or plans to take, corrective action to address all the control issues we identified. We plan to follow up on the status of BPD's actions to address the issues identified as part of our fiscal year 2007 Schedule of Federal Debt audit.

Recommendation for Executive Action

We recommend that the Commissioner of the Bureau of the Public Debt direct the appropriate BPD officials to implement the eight new detailed recommendations set forth in the separately issued Limited Official Use Only version of this report.

Agency Comments and Evaluation

BPD provided comments on the detailed findings and recommendations in the Limited Official Use Only version. In those comments, the Commissioner of the Bureau of the Public Debt stated that of the 11 recommendations, which include 3 from a prior year, 4 have been completely resolved, and corrective actions for the remaining 7 are in progress. The Commissioner also stated that BPD intends to fully implement the remaining recommendations by May 2008. We have modified our Limited Official Use Only version of this report to acknowledge, where appropriate, BPD's comments concerning additional actions taken in accordance with our recommendations. Also, we plan to follow up on these matters during our audit of the fiscal year 2007 Schedule of Federal Debt.

- - - - -

In the separately issued Limited Official Use Only report, we noted that the head of a federal agency is required by 31 U.S.C. 720 to submit a written statement on actions taken on our recommendations to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on Oversight and Government Reform not later than 60 days after the date of the Limited Official Use Only report. A written statement must also be sent to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of that report. In the Limited Official Use Only report, we also requested a copy of your responses.

We are sending copies of this report to the Chairmen and Ranking Minority Members of the Senate Committee on Homeland Security and Governmental Affairs; the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Senate Committee on Homeland Security and Governmental Affairs; the Subcommittee on Financial Services and General Government, Senate Committee on Appropriations; the House Committee on Oversight and Government Reform; the Subcommittee on Government Management, Organization, and Procurement, House Committee on Oversight and Government Reform; and the Subcommittee on Financial Services and General Government, House Committee on Appropriations. We are also sending copies of this report to the Secretary of the Department of the Treasury, the Acting Inspector General of the Department of the Treasury, 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 me at (202) 512-3406 or engelg@gao.gov. Other key contributors to this assignment were Jeff L. Knott and Dawn B. Simpson, Assistant Directors, Dean D. Carpenter, and Debra M. Conner.

Sincerely yours,

Gary T. Engel

Gary T. Engel
Director
Financial Management and Assurance

(198513)