



GAO

Accountability \* Integrity \* Reliability

United States Government Accountability Office  
Washington, DC 20548

April 28, 2009

The Honorable Van Zeck  
Commissioner  
Bureau of the Public Debt

**On April 29, 2009, GAO revised this product to clarify the scope and focus of BPD's compensating controls with respect to detecting potential misstatements in the Schedule of Federal 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,<sup>1</sup> 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, 2008 and 2007.<sup>2</sup> As part of these audits, we performed a review of the general and application information security controls over key BPD financial systems.

As we reported in connection with our audit of the Schedules of Federal Debt for the fiscal years ended September 30, 2008 and 2007, 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, 2008, 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. However, we found deficiencies involving information security controls that we do not consider to be significant deficiencies.<sup>3</sup> With regard to financial reporting and compliance with applicable laws and regulations, BPD mitigated the potential effect of such control deficiencies with physical security measures, a program of monitoring user and system activity, and compensating management and reconciliation controls. Nevertheless, these matters warrant BPD management's attention and action.

---

<sup>1</sup>31 U.S.C. § 331(e).

<sup>2</sup>GAO, *Financial Audit: Bureau of the Public Debt's Fiscal Years 2008 and 2007 Schedules of Federal Debt*, GAO-09-44 (Washington, D.C.: Nov. 7, 2008).

<sup>3</sup>A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with U.S. generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. A control deficiency exists when the design or operation of a control does not allow management or employees in the normal course of performing their assigned functions to prevent or detect misstatements on a timely basis.

This report presents the control deficiencies we identified during our fiscal year 2008 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 address recommendations that were contained in our prior years' audit reports and open as of September 30, 2007. 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 will issue a separate report to the Board of Governors of the Federal Reserve System on the results from that assessment.

## **Results in Brief**

Our fiscal year 2008 audit procedures identified three new general information security control deficiencies, related to access control and incident response. In the Limited Official Use Only report, we made three recommendations to address these control deficiencies.

None of the control deficiencies we identified represented significant risks to the BPD financial systems. With regard to financial reporting and compliance with applicable laws and regulations, BPD mitigated the potential effect of such control deficiencies with physical security measures and a program of monitoring user and system activity. Further, BPD has compensating management and reconciliation controls that are designed to detect potential misstatements in the Schedule of Federal Debt.

During our follow-up on the status of BPD's corrective actions to address 13 open recommendations related to general information security control deficiencies identified in prior years' audits for which actions were not complete as of September 30, 2007, we determined the following:

- As of September 30, 2008, corrective action on 8 of the 13 recommendations was completed.
- Corrective action was in progress as of September 30, 2008, on the five remaining open recommendations, two of which relate to system software and the other three to application software development and change control.

BPD provided comments on the detailed findings and recommendations in the separately issued Limited Official Use Only report. In those comments, the Commissioner of BPD stated that of the eight findings that were open as of September 30, 2008, four have been completely resolved, and corrective actions for the remaining four are in progress. The Commissioner also stated that BPD intends to implement corrective actions for three of the four remaining findings by September 2009, and develop a plan to address the other remaining finding by December 2009.

## Background

The Department of the Treasury (Treasury) is authorized by Congress to borrow money backed by the faith and 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 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, 2008 and 2007, federal debt managed by BPD totaled about \$10.0 trillion and \$9.0 trillion, respectively, for moneys borrowed to fund the government's operations. These balances consisted of approximately (1) \$5.8 trillion and \$5.1 trillion of debt held by the public as of September 30, 2008 and 2007, respectively, and (2) \$4.2 trillion and \$3.9 trillion of intragovernmental debt holdings as of September 30, 2008 and 2007, respectively. Total interest expense on federal debt managed by BPD for fiscal years 2008 and 2007 was about \$454 billion and \$433 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. FRBs use a number of financial systems to process debt-related transactions. 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 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, 2007. We use a risk-based, rotation approach for testing general information security controls. Each general information security control area is subjected to a more detailed 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*.<sup>4</sup> Areas considered to be of higher risk are subject to more frequent review. Each key application is subjected to a 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 adequately designed, implemented, and operating effectively.

---

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

The scope of our work for fiscal year 2008 as it relates to general information security controls included following up on open recommendations from our prior years' reports and reviewing access control, system software, segregation of duties, and incident response. In addition, we performed security diagnostics and vulnerability assessment testing of BPD's internal and external information system environment.

Application information security control reviews were performed on six key BPD applications to determine whether the applications are designed to provide reasonable assurance 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.

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 seven key financial applications maintained and operated by the FRBs.

The evaluation and testing of certain information security controls, including the follow-up on the status of BPD corrective actions to address open recommendations from our prior years' reports, 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 determine 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 deficiencies identified. We plan to follow up on corrective actions taken for these matters during our audit of the fiscal year 2009 Schedule of Federal Debt.

We performed our work at the BPD data center from March 2008 through October 2008. Our work was performed in accordance with U.S. generally accepted government auditing standards. As noted above, 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 an entitywide security management program, access controls, system software controls, application software development and change controls, 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 2008 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 three new general information security control deficiencies. This included one control deficiency related to logical access control and two control deficiencies related to incident response.

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.

Incident response capability refers to the organization's ability to prevent, detect, and respond to malicious technical threats to its systems. If successful, these security incidents can place valuable resources at risk of corruption or disclosure. An organization's incident response capability is intended to contain and repair damages as well as prevent future damages from incidents.

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

During our follow-up on the status of BPD's corrective actions to address 13 open recommendations related to general information security control deficiencies identified in prior years' audits for which actions were not complete as of September 30, 2007, we determined the following:

- As of September 30, 2008, corrective action on 8 of the 13 recommendations was completed.
- Corrective action was in progress as of September 30, 2008, on the five remaining open recommendations, two of which relate to system software and the other three to application software development and change control. Although BPD management has made progress in addressing the remaining five general information security control deficiencies, additional actions are still needed.

None of the control deficiencies we identified represented significant risks to the BPD financial systems. With regard to financial reporting and compliance with applicable laws and regulations, BPD mitigated the potential effect of such control deficiencies with physical security measures and a program of monitoring user and system activity. Further, BPD has compensating management and reconciliation controls that are designed to detect potential misstatements in the Schedule of Federal Debt. 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. We will issue a separate report to the Board of Governors of the Federal Reserve System on the results from that assessment.

### **Conclusion**

BPD has made significant progress in addressing open information security control recommendations from our prior years' audits and is taking corrective action to address but has not yet completed all required actions on the five remaining unresolved control deficiencies.

Our fiscal year 2008 audit also identified three new general information security control deficiencies, related to access control and incident response. For these identified control deficiencies, we are making three recommendations. BPD informed us that it has taken or plans to take corrective action to address all the control deficiencies identified.

### **Recommendation for Executive Action**

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

## Agency Comments and Our Evaluation

BPD provided comments on the detailed findings and recommendations in the Limited Official Use Only version. In those comments, the Commissioner of BPD stated that of the eight findings that were open as of September 30, 2008, four have been completely resolved, and corrective actions for the remaining four are in progress. The Commissioner also stated that BPD intends to implement corrective actions for three of the four remaining findings by September 2009, and develop a plan to address the other remaining finding by December 2009. We plan to follow up on corrective actions taken for these matters during our audit of the fiscal year 2009 Schedule of Federal Debt.

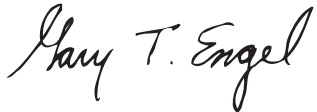
-----

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 interested congressional committees, the Secretary of the Treasury, the Inspector General of the Department of the Treasury, and the Director of the Office of Management and Budget. In addition, this report is available at no charge on the GAO 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](mailto:engelg@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are Jeffrey L. Knott and Dawn B. Simpson, Assistant Directors; Dean D. Carpenter; and Zsaroq R. Powe.

Sincerely yours,



Gary T. Engel  
Director  
Financial Management and Assurance

(198562)

---

---

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

---



---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site ([www.gao.gov](http://www.gao.gov)). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to [www.gao.gov](http://www.gao.gov) and select "E-mail Updates."

---

## Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office  
441 G Street NW, Room LM  
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000  
TDD: (202) 512-2537  
Fax: (202) 512-6061

---

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

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto:dawnr@gao.gov), (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548