



GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 26, 2010

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, 2009 and 2008.² 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, 2009 and 2008, we concluded that BPD maintained, in all material respects, effective internal control over financial reporting relevant to the Schedule of Federal Debt as of September 30, 2009, that provided reasonable assurance that misstatements, losses, or noncompliance material in relation to the Schedule of Federal Debt would be prevented or detected and corrected on a timely basis. However, we identified information security deficiencies affecting internal control over financial reporting, which, while we do not consider them to be collectively either a material weakness or significant deficiency, nevertheless warrant BPD management's attention and action.³

This report presents the control deficiencies we identified during our fiscal year 2009 testing of the general and application information security controls that support key

¹31 U.S.C. § 331(e).

²GAO, *Financial Audit: Bureau of the Public Debt's Fiscal Years 2009 and 2008 Schedules of Federal Debt*, GAO-10-88 (Washington, D.C.: Nov. 10, 2009).

³A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A deficiency in internal control 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 and correct misstatements on a timely basis.

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 information security control-related recommendations contained in our prior years' audit reports and open as of September 30, 2008. 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 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 2009 audit procedures identified seven new general information security control deficiencies related to access controls and configuration management. In the Limited Official Use Only report, we made eight recommendations to address these control deficiencies.

None of the control deficiencies we identified represented significant risks to the BPD financial systems. The potential effect of such control deficiencies on financial reporting relevant to the Schedule of Federal Debt was mitigated by BPD's physical security measures and a program of monitoring user and system activity, as well as compensating management and reconciliation controls designed to detect potential misstatements in the Schedule of Federal Debt.

In addition, during our fiscal year 2009 follow-up on the status of BPD's corrective actions to address eight open recommendations related to general information security control deficiencies identified in prior years' audits, we determined that as of September 30, 2009, corrective action on five of the eight recommendations was completed, while corrective action was in progress on the three remaining open recommendations, which related to access controls and configuration management.

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 10 findings open as of September 30, 2009, 3 have been completely resolved and corrective actions for the remaining 7 are planned or in progress. The Commissioner also stated that BPD intends to implement corrective actions for 5 of the 7 remaining findings by September 2010, and the other 2 by December 2011.

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, 2009 and 2008, federal debt managed by BPD totaled about \$11.9 trillion and \$10.0 trillion, respectively, primarily for moneys borrowed to fund the government's operations. These balances consisted of approximately (1) \$7.6 trillion and \$5.8 trillion of debt held by the public as of September 30, 2009 and 2008, respectively, and (2) \$4.3 trillion and \$4.2 trillion of intragovernmental debt holdings as of September 30, 2009 and 2008, respectively. Total interest expense on federal debt managed by BPD for fiscal years 2009 and 2008 was about \$381 billion and \$454 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, 2008. Our evaluation of the general and application information security controls was conducted using the *Federal Information System Controls Audit Manual*.⁴

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.

The scope of our general information security controls work for fiscal year 2009 as it relates to general information security controls included following up on open recommendations from our prior years' reports and testing all five general control areas (security management, access controls, configuration management, segregation of duties, and contingency planning) in the current year. In addition, we performed security diagnostics and vulnerability assessment testing of BPD's internal and external information system environment.

⁴GAO, *Federal Information System Controls Audit Manual*, GAO-09-232G (Washington, D.C.: February 2009).

We performed application information security control reviews on six key BPD applications to determine whether the applications were designed to provide reasonable assurance that

- all transactions that occurred were input into the system, accepted for processing, processed once and only once by the system, and properly included in output;
- transactions were properly recorded in the proper period, key data elements input for transactions were accurate, data elements were processed accurately by applications that produce reliable results, and output was accurate;
- all recorded transactions actually occurred, related to the organization, and were properly approved in accordance with management's authorization, and output contained only valid data;
- application data and reports and other output were protected against unauthorized access; and
- application data and reports and other relevant business information were readily available to users when needed.

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 four 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. We plan to follow up to determine the status of corrective actions taken for matters open as of September 30, 2009, during our audit of the fiscal year 2010 Schedule of Federal Debt.

We performed our work at the BPD data center from February 2009 through October 2009. Our work was performed in accordance with U.S. generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

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.

New Areas for Improvement in BPD's General 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 security management, access controls, configuration management, segregation of duties, and contingency planning. An effective general information security control environment (1) provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls to ensure that an adequate security management program is in place; (2) limits or detects access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure; (3) prevents unauthorized changes to information system resources (for example, software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended; (4) includes policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations; and (5) protects critical and sensitive data, and provides for critical operations to continue without disruption or be promptly resumed when unexpected events occur.

Our fiscal year 2009 testing identified opportunities to strengthen certain information security controls that support key BPD financial systems relevant to BPD's Schedule of Federal Debt. Specifically, our audit procedures identified seven new general information security control deficiencies. This included five control deficiencies related to logical access controls and two control deficiencies related to configuration management.

Access controls are important because they limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure. Such controls include logical access controls and physical access controls. The new access control deficiencies we identified related to logical access controls. Logical access controls require users to authenticate themselves through the use of secret passwords or other identifiers, and limit the files and other resources that authenticated users can access and the actions that they can execute.

Configuration management is important because it involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. At each system sublevel (for example, network, operating systems, and infrastructure applications),

configuration management controls ensure that only authorized changes are made to such critical components. In addition, configuration management controls ensure applications and changes to the applications go through a formal, documented systems development process that identifies all changes to the baseline configuration.

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

In addition, during our fiscal year 2009 follow-up on the status of BPD's corrective actions to address eight open recommendations related to general information security control deficiencies identified in prior years' audits, we determined that as of September 30, 2009, corrective action on five of the eight recommendations was completed, while corrective action was in progress on the three remaining open recommendations, which related to access controls and configuration management. Although BPD management has made progress in addressing the remaining three 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. The potential effect of such control deficiencies on financial reporting relevant to the Schedule of Federal Debt was mitigated by BPD's physical security measures and a program of monitoring user and system activity, as well as compensating management and reconciliation controls designed to detect potential misstatements in the Schedule of Federal Debt. Nevertheless, these deficiencies warrant management's attention and action to limit the risk of unauthorized access, loss, or disclosure; 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 while actions are still needed in three control areas, it has corrective actions underway or planned. Our fiscal year 2009 audit also identified seven new general information security control deficiencies related to access controls and configuration management.

Recommendations 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 presented in the separately issued Limited Official Use Only version of this report.

Agency Comments and Our Evaluation

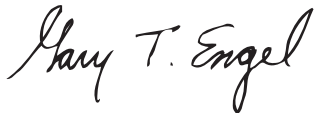
BPD provided comments on the detailed findings and recommendations in the separately issued Limited Official Use Only report. In those comments, the Commissioner of BPD stated that of the 10 findings open as of September 30, 2009, 3 have been completely resolved and corrective actions for the remaining 7 are planned or in progress. The Commissioner also stated that BPD intends to implement corrective actions for 5 of the 7 remaining findings by September 2010, and the other 2 by December 2011. We plan to follow up to determine the status of corrective actions taken for these matters during our audit of the fiscal year 2010 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 Senate and House 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. 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 Nicole N. Jarvis.

Sincerely yours,



Gary T. Engel
Director
Financial Management and Assurance

(198605)

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). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

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

Congressional Relations

Ralph Dawn, Managing Director, 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, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548