



GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 16, 2006

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, 2005 and 2004.² 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, 2005 and 2004, 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, 2005, 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 conditions³ but that nevertheless warrant BPD management's attention and action. BPD mitigates 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 results of our fiscal year 2005 testing of the general and application information security controls that support key BPD automated financial systems relevant to BPD's Schedule of Federal Debt and the results of our follow-up

¹31 U.S.C. § 331(e).

²GAO, *Financial Audit: Bureau of the Public Debt's Fiscal Years 2005 and 2004 Schedules of Federal Debt*, GAO-06-169 (Washington, D.C.: Nov. 7, 2005).

³Reportable 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.

on the status of BPD's corrective actions to address recommendations that were contained in our prior years' audits and open as of September 30, 2004. 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 of such testing.

Results in Brief

Our fiscal year 2005 audit procedures 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 11 new general information security control issues that relate to access controls and system software. In the Limited Official Use Only report, we made nine recommendations to address these issues.

Our follow-up on the status of BPD's corrective actions to address nine open recommendations related to eight general and application information security control issues identified in prior years' audits for which actions were not complete as of September 30, 2004, identified the following:

- As of September 30, 2005, corrective action on seven of the nine recommendations had been completed.
- Corrective action was in progress as of September 30, 2005, on the two remaining open recommendations, which relate to access controls and application controls. We reaffirm our prior years' recommendations related to these issues.

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 the Public Debt stated that of the 11 recommendations, which include 2 from prior years, 5 have been completely resolved, and the remaining 6 are in progress. The Commissioner also stated that BPD intends to fully implement the remaining recommendations before the end of this fiscal year.

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, 2005 and 2004, federal debt managed by BPD totaled about \$7.9 trillion and \$7.4 trillion, respectively, for moneys borrowed to fund the government's operations. These balances consisted of approximately (1) \$4.6 trillion and \$4.3 trillion of debt held by the public as of September 30, 2005 and 2004, respectively; and (2) \$3.3 trillion and \$3.1 trillion of intragovernmental debt holdings as of September 30, 2005 and 2004, respectively. Total interest expense on federal debt managed by BPD for fiscal years 2005 and 2004 was about \$355 billion and \$322 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.

Objectives, Scope, and Methodology

Our objectives were to evaluate and test 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, 2004. 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 every year to a full-scope review.

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 2005 as it relates to general information security controls included following up on open recommendations from our prior years' reports and reviewing entitywide security program planning and management, access

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

controls, and system software controls. In addition, we performed certain testing of the BPD distributed computing environment.

We performed full-scope application information security control reviews of 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.

We performed a limited application information security control review of one key BPD application to expand our understanding of this new application. 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, 2004. 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 certain information security controls were performed by the independent public accounting (IPA) firm of PricewaterhouseCoopers 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. In addition, our information systems auditors performed supplemental testing of general and application information security controls at BPD and followed up on the status of BPD corrective actions to address certain open recommendations in our fiscal year 2004 report.

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 identified. We plan to follow up on these matters during our audit of the fiscal year 2006 Schedule of Federal Debt.

We performed our work at the BPD data center from February 2005 through October 2005. 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 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 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 2005 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 11 new general information security control issues. Ten new general information security control issues relate to access controls and one new general information security control issue relates to system software. The majority of the new issues involves controls pertaining to the distributed computing environment.

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. Physical access controls involve the use of locks, guards, badges, alarms, and similar measures (used alone or in combination) to prevent intentional or unintentional loss or impairment to computer hardware and software and to the buildings and rooms where they are housed.

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.

In a separately issued Limited Official Use Only report, we communicated detailed information regarding our findings to BPD management and made nine recommendations to address the access control and system software issues.

Our follow-up on the status of BPD's corrective actions to address nine open recommendations related to eight general and application information security control issues identified in prior years' audits for which actions were not complete as of September 30, 2004, found the following:

- As of September 30, 2005, corrective action on seven of the nine recommendations had been completed.
- Corrective action was in progress as of September 30, 2005, on the two remaining open recommendations, which relate to access controls and application controls. We reaffirm our prior years' recommendations related to these issues.

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. We will issue a separate report to the Board of Governors of the Federal Reserve System on the results of such testing.

Conclusion

BPD has made significant progress in addressing open recommendations from our prior years' audits and is taking corrective action to address the two remaining unresolved issues. We therefore reaffirm our two recommendations related to these issues.

Our fiscal year 2005 audit identified 11 new general information security control issues that relate to access controls and system software for which we are making 9 recommendations. BPD informed us that it has taken or plans to take corrective action to address all issues 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 nine 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 the Bureau of the Public Debt stated that of the 11 recommendations, which include 2 from prior years, 5 have been completely resolved, and the remaining 6 are in progress. The Commissioner also stated that BPD intends to fully implement the remaining recommendations before the end of this fiscal year. We plan to follow up on these matters during our audit of the fiscal year 2006 Schedule of Federal Debt.

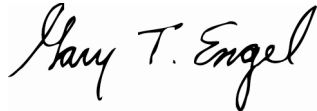
In the separately issued Limited Official Use Only report, we noted that the head of a federal agency is required by 31 U.S.C. 720 to submit a written statement on actions taken on our recommendations to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on 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, and International Security, Senate Committee on Homeland Security and Governmental Affairs; the Subcommittee on Transportation, Treasury, the Judiciary, Housing and Urban Development, and Related Agencies, Senate Committee on Appropriations; the House Committee on Government Reform; the Subcommittee on Government Management, Finance, and Accountability, House Committee on Government Reform; and the Subcommittee on Transportation, Treasury, and Housing and Urban Development, The Judiciary, District of Columbia, House Committee on Appropriations. We are also sending copies of this report to the Secretary of the Department of the Treasury, the 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 David B. Hayes and Dawn B. Simpson, Assistant Directors; and Angela M. Bell, Bruce E. Cain, and Mickie E. Gray.

Sincerely yours,

A handwritten signature in cursive script that reads "Gary T. Engel".

Gary T. Engel
Director
Financial Management and Assurance

(198417)

This is a work of the U.S. government and is not subject to copyright protection in the United States. It 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, 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 and select "Subscribe to 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, D.C. 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

E-mail: fraudnet@gao.gov

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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548