GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

May 24, 2012

The Honorable Van Zeck
Commissioner
Bureau of the Public Debt

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

Dear Mr. Zeck:

In connection with fulfilling our requirement to audit the consolidated 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, 2011 and 2010.[2] As part of these audits, we performed a review of information systems 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, 2011 and 2010, 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, 2011, 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 systems 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 the attention and action of management.[3]

---

[1]31 U.S.C. § 331(e)(2). As a bureau within the Department of the Treasury, federal debt and related activity and balances are also significant to the consolidated financial statements of the Department of the Treasury (see 31 U.S.C. § 3515(b)).

[2]GAO, *Financial Audit: Bureau of the Public Debt's Fiscal Years 2011 and 2010 Schedules of Federal Debt*, GAO-12-164 (Washington, D.C.: Nov. 8, 2011).

[3]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 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 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.

This report presents the deficiencies we identified during our fiscal year 2011 testing of information systems controls over key BPD financial systems relevant to the 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 systems control-related recommendations contained in our prior years' reports and open as of September 30, 2010. We also assessed information systems controls over key financial systems maintained and operated by the Federal Reserve Banks (FRB) on behalf of BPD relevant to the Schedule of Federal Debt. We issued a separate report to the Board of Governors of the Federal Reserve System on the results from that assessment.

Results in Brief

During our fiscal year 2011 audit, we identified eight new general information systems control deficiencies related to access controls, configuration management, and segregation of duties. We made nine recommendations to address these control deficiencies. In a separately issued Limited Official Use Only report, we communicated to BPD management detailed information regarding our findings and related recommendations.

None of the control deficiencies we identified represented significant risks to the BPD financial systems. The potential effect of these deficiencies on the Schedule of Federal Debt financial reporting 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 2011 follow-up on the status of BPD's corrective actions to address information systems control-related recommendations contained in our prior years' reports and open as of September 30, 2010, we determined that corrective action was complete for one of the eight open recommendations and corrective action was in progress for each of the seven remaining open recommendations related to access controls, configuration management, and segregation of duties.

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, subsequent to September 30, 2011, four of the five unresolved general information systems control deficiencies contained in our prior years' reports have been completely resolved and one has been substantially addressed with BPD accepting the residual risk. The Commissioner also cited actions taken or planned to address the eight new general information systems control deficiencies.

Background

The Department of the Treasury (Treasury) is authorized by Congress to borrow money backed by the full 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 maintains an investment program for federal government accounts, including trust funds, that have legislative authority to invest temporary cash reserves not needed for current benefits and expenses.

As of September 30, 2011 and 2010, federal debt managed by BPD totaled about $14.8 trillion and $13.5 trillion, respectively, primarily for moneys borrowed to fund the federal government's operations. These balances consisted of approximately (1) $10.1 trillion and $9.0 trillion of debt held by the public as of September 30, 2011 and 2010, respectively, and (2) $4.7 trillion and $4.5 trillion of intragovernmental debt holdings as of September 30, 2011 and 2010, respectively. Total interest expense on federal debt managed by BPD for fiscal years 2011 and 2010 was about $454 billion and $413 billion, respectively.

BPD relies on a number of interconnected financial systems and electronic data to process and track the money that it borrows and to account for the securities it issues. Many of the FRBs provide fiscal agent services on behalf of BPD. Such services 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 key 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.

General information systems controls are the structure, policies, and procedures that apply to an entity's overall computer operations. General information systems controls establish the environment in which the application systems and controls operate. They include five general control areas—security management, access controls, configuration management, segregation of duties, and contingency planning.[4] An effective general information systems 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 (security management); (2) limits or detects access to computer resources such as data, programs, equipment, and facilities, thereby protecting them against unauthorized modification, loss, and disclosure (access controls); (3) prevents unauthorized changes to information system resources, such as software programs and hardware configurations, and provides reasonable assurance that systems are configured and operating securely and as intended (configuration management); (4) includes policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations (segregation of duties); and (5) protects critical and sensitive data, and provides for critical operations to continue without disruption or be promptly resumed when unexpected events occur (contingency planning).

[4]GAO, *Government Auditing Standards*, GAO-07-731G (Washington, D.C.: July 2007), 135.

Objectives, Scope, and Methodology

Our objectives were to evaluate information systems controls over key financial systems maintained and operated by, and on behalf of, BPD that are relevant to the Schedule of Federal Debt, and to determine the status of BPD's corrective actions to address information systems control-related recommendations in our prior years' reports for which actions were not complete as of September 30, 2010. Our evaluation of information systems controls was conducted using the Federal Information System Controls Audit Manual (FISCAM).[5]

To evaluate information systems controls, we identified and reviewed BPD's information systems 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 systems controls work for fiscal year 2011 included (1) following up on open recommendations from our prior years' reports and (2) using a risk-based approach to testing the five general control areas related to the systems in which the applications operate and other critical control points in the systems or networks that could impact the effectiveness of the information systems controls at BPD in the current year. In addition, we assessed software and network security by reviewing vulnerability scans and penetration testing performed by BPD over key BPD financial systems relevant to the Schedule of Federal Debt.

We determined whether relevant application controls were appropriately designed and implemented, and then performed tests to determine whether the application controls were operating effectively. We reviewed five key BPD applications relevant to the Schedule of Federal Debt to determine whether the application controls were designed and operating effectively 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.

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

We also reviewed the application information systems control audit documentation from the work performed by the Treasury Office of Inspector General's contractor on two other key BPD applications.

Because the FRBs are integral to the operations of BPD, we evaluated information systems controls over key financial systems maintained and operated by the FRBs on behalf of BPD that are relevant to the Schedule of Federal Debt, and determined the status of FRBs' corrective actions to address information systems control-related recommendations contained in our prior years' reports for which actions were not complete as of September 30, 2010. This included using a risk-based approach to testing the five general control areas related to the systems in which the applications operate and other critical control points in the systems or networks that could impact the effectiveness of the information systems controls at the relevant FRBs. We also evaluated the relevant application controls over four applications maintained and operated by the FRBs.

The independent public accounting (IPA) firm of Cotton and Company LLP evaluated and tested certain BPD information systems controls, including the follow-up on the status of BPD's corrective actions during fiscal year 2011 to address open recommendations from our prior years' reports. 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 firm's 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, 2011, during our audit of the fiscal year 2012 Schedule of Federal Debt.

We performed our work at the BPD data center where the operations of the systems we reviewed are supported. Our work was performed from February 2011 through October 2011 in accordance with U.S. generally accepted government auditing standards. We believe that our audit provided a reasonable basis for our conclusions in this report.

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 on the draft Limited Official Use Only report are summarized in the Agency Comments and Our Evaluation section of this report.

Assessment of BPD's Information Systems Controls

During our fiscal year 2011 testing, we identified opportunities to strengthen certain information systems controls that support key BPD financial systems relevant to BPD's Schedule of Federal Debt. Specifically, we identified eight new general information systems control deficiencies related to access controls, configuration management, and segregation of duties. Additionally, BPD had an open Plan of Action and Milestones related to self-identified information security deficiencies that we considered in determining that there was not a material weakness or significant deficiency in BPD's internal control.

Access controls are important because they limit access 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 during fiscal year 2011 related to logical access controls. Effectively designed and implemented logical access controls require users to authenticate themselves through the use of passwords or other identifiers, and limit the files and other resources that authenticated users can access and the actions that they can execute based on a valid need that is determined by assigned official duties.

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. Patch management, a component of configuration management, is an important element in mitigating the risks associated with software vulnerabilities. Effectively designed and implemented configuration management controls provide reasonable assurance that only authorized changes are made to critical components at each system sublevel (i.e., network, operating systems, and infrastructure applications). In addition, effectively designed and implemented configuration management controls provide reasonable assurance that applications and changes to the applications go through a formal, documented systems development process that identifies all changes to the baseline configuration.

Segregation of duties is important because work responsibilities should be segregated so that one individual does not control all critical stages of a process. An effective segregation of duties is achieved by splitting responsibilities between two or more organizational groups. In addition, dividing duties this way diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.

In a separately issued Limited Official Use Only report, we communicated to BPD management detailed information regarding the eight new general information systems control deficiencies and made nine recommendations to address these control deficiencies.

In addition, our fiscal year 2011 follow-up on the status of actions taken by BPD to address previously identified, but unresolved, general information systems control deficiencies as of September 30, 2010, found that corrective action was complete for one of the eight open recommendations and corrective action was in progress for each of the seven remaining open recommendations related to access controls, configuration management, and segregation of duties.

None of the control deficiencies we identified represented significant risks to the BPD financial systems. The potential effect of these deficiencies on the Schedule of Federal Debt financial reporting 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 increase the risk of unauthorized access, loss, modification, or disclosure of sensitive data and programs and disruption of critical operations and, therefore, warrant the attention and action of management.

Conclusion

Our fiscal year 2011 audit identified eight new general information systems control deficiencies related to access controls, configuration management, and segregation of duties. Furthermore, while BPD has corrective actions under way or planned, additional actions are needed to fully address the open information systems control recommendations from our prior years' audits related to access controls, configuration management, and segregation of duties. Until these information systems control deficiencies are fully addressed, there will be an increased risk of unauthorized access, loss, modification, or disclosure of sensitive data and programs and disruption of critical operations. We will follow up to determine the status of BPD's actions taken in response to these open recommendations during our audit of the fiscal year 2012 Schedule of Federal Debt.

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, subsequent to September 30, 2011, four of the five unresolved general information systems control deficiencies contained in our prior years' reports have been completely resolved and one has been substantially addressed with BPD accepting the residual risk. The Commissioner also stated that of the eight new general information systems control deficiencies, five have been completely resolved as of the date of his letter and that for the three remaining new deficiencies, the Commissioner stated that BPD intends to (1) implement corrective actions to address one by August 2012 and another by July 2013, and (2) develop a plan for implementing corrective actions for the remaining deficiency by December 2012. We plan to follow up to determine the status of corrective actions taken for these matters during our audit of the fiscal year 2012 Schedule of Federal Debt.

- - - - -

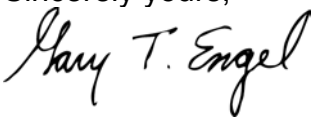
In the separately issued Limited Official Use Only report, we noted that the head of a federal agency is required by 31 U.S.C. § 720 to submit a written statement on actions taken on our recommendations to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on 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 Acting Director of the Office of Management and Budget. This report also is available at no charge on the GAO's Website 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 include Jeffrey L. Knott and Dawn B. Simpson, Assistant Directors; Nicole N. Jarvis; Nicole M. McGuire; and Seong Bin Park.

Sincerely yours,



Gary T. Engel
Director
Financial Management and Assurance

(198697)