Audit Report

OIG-07-044

Report on Controls Placed In Operation and Tests of Operating Effectiveness for the Bureau of the Public Debt's Administrative Resource Center for the Period July 1, 2006 to June 30, 2007

August 17, 2007

Office of Inspector General

Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

August 16, 2007

MEMORANDUM FOR VAN ZECK, COMMISSIONER
BUREAU OF THE PUBLIC DEBT

FROM: Michael Fitzgerald Michael Fitzgerald
Director, Financial Audits

SUBJECT: Report on Controls Placed in Operation and Tests of Operating Effectiveness for the Bureau of the Public Debt's Administrative Resource Center for the Period July 1, 2006 to June 30, 2007

I am pleased to transmit the attached Report on Controls Placed in Operation and Tests of Operating Effectiveness for the Bureau of the Public Debt's (BPD) Administrative Resource Center for the period July 1, 2006 to June 30, 2007. Under a contract monitored by the Office of Inspector General, KPMG LLP, an independent certified public accounting firm, performed an examination of the accounting processing and general computer controls related to certain services provided by BPD's Administrative Resource Center to various Federal Government agencies (Customer Agencies) for the period July 1, 2006 to June 30, 2007. The contract required that the examination be performed in accordance with generally accepted government auditing standards and the American Institute of Certified Public Accountants' Statement on Auditing Standards Number 70, *Reports on the Processing of Transactions by Service Organizations*, as amended.

The following reports, prepared by KPMG LLP, are incorporated in the attachment:

- Independent Service Auditors' Report; and
- Independent Auditors' Report on Compliance with Laws and Regulations.

In its examination of the BPD's Administrative Resource Center, KPMG LLP found:

- the *Description of Controls Provided by the BPD* presents fairly, in all material respects, the relevant aspects of BPD's controls that had been placed in operation as of June 30, 2007,
- that these controls are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and Customer Agencies and sub-service organizations applied the controls contemplated in the design of BPD's controls,

- that the controls tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period from July 1, 2006 to June 30, 2007, and
- no instances of reportable noncompliance with laws and regulations tested.

In connection with the contract, we reviewed KPMG LLP's reports and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on BPD's description of controls, the suitability of the design of these controls and the operating effectiveness of controls tested or a conclusion on compliance with laws and regulations. KPMG LLP is responsible for the attached auditors' reports dated July 20, 2007 and the conclusions expressed in the reports. However, our review disclosed no instances where KPMG LLP did not comply, in all material respects, with generally accepted government auditing standards.

Should you have any questions, please contact me at (202) 927-5789, or a member of your staff may contact Mark S. Levitt, Audit Manager, Financial Audits at (202) 927-5076.

Attachment

U.S. Department of the Treasury
Bureau of the Public Debt

Administrative Resource Center Financial Management Services Accounting Processing and General Computer Controls

Report on Controls Placed in Operation and Tests of Operating Effectiveness For the Period July 1, 2006 to June 30, 2007

U.S. DEPARTMENT OF THE TREASURY
BUREAU OF THE PUBLIC DEBT
ADMINISTRATIVE RESOURCE CENTER
FINANCIAL MANAGEMENT SERVICES

REPORT ON CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

Table of Contents

I. INDEPENDENT SERVICE AUDITORS' REPORT PROVIDED BY KPMG LLP

KPMG LLP
2001 M Street, NW
Washington, DC 20036

Independent Service Auditors' Report

Inspector General, U.S. Department of the Treasury
Deputy Executive Director, Administrative Resource Center

We have examined the accompanying description of the accounting processing and general computer controls related to the financial management services provided by the Administrative Resource Center (ARC) of the Bureau of the Public Debt (BPD). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of BPD's controls that may be relevant to a Customer Agencies' internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and Customer Agencies and sub-service organizations applied the controls contemplated in the design of BPD's controls; and (3) such controls had been placed in operation as of June 30, 2007. BPD uses services provided by other organizations external to BPD (sub-service organizations). A list of sub-service organizations is provided in Section II of this report. The accompanying description includes only those controls and related control objectives of BPD, and does not include control objectives and related controls of sub-service organizations. Our examination did not extend to controls of sub-service organizations. The control objectives were specified by the management of BPD. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and applicable *Government Auditing Standards* issued by the Comptroller General of the United States and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of BPD's controls that had been placed in operation as of June 30, 2007. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and Customer Agencies and sub-service organizations applied the controls contemplated in the design of BPD's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Section III, to obtain evidence about their effectiveness in meeting the control objectives, described in Section III, during the period from July 1, 2006 to June 30, 2007. The specific controls and the nature, timing, extent, and results of the tests are listed in Section III. This information is being provided to Customer Agencies of BPD and to their auditors to be taken into consideration, along with information about the internal control of Customer Agencies, when making assessments of control risk for Customer Agencies. In our opinion, the controls that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section III were achieved during the period from July 1, 2006 to June 30, 2007.

The relative effectiveness and significance of specific controls at BPD and their effect on assessments of control risk at Customer Agencies are dependent on their interaction with the controls, and other factors present at individual Customer Agencies. We have performed no procedures to evaluate the effectiveness of controls at individual Customer Agencies.

The description of controls at BPD is as of June 30, 2007, and the information about tests of the operating effectiveness of specific controls covers the period from July 1, 2006 to June 30, 2007. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at BPD is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes made to the system or controls, or the failure to make needed changes to the system or controls may alter the validity of such conclusions.

The information in Section IV of this report is presented by BPD to provide additional information and is not a part of BPD's description of controls placed in operation. The information in Section IV has not been subjected to the procedures applied in the examination of the description of the controls applicable to the processing of transactions for Customer Agencies and, accordingly, we express no opinion on it.

This report is intended solely for the information and use of the management of BPD, its Customer Agencies, the independent auditors of its Customer Agencies, the U.S. Department of the Treasury Office of Inspector General, the Office of Management and Budget, the Government Accountability Office, and the U.S. Congress, and is not intended to be, and should not be, used by anyone other than these specified parties.

KPMG LLP

July 20, 2007

II. DESCRIPTION OF CONTROLS PROVIDED BY THE BUREAU OF THE PUBLIC DEBT

OVERVIEW OF OPERATIONS

The Bureau of the Public Debt's (BPD's) Administrative Resource Center (ARC) has been a member of the Treasury Franchise Fund (TFF) since August 1998. The TFF was established by P.L. 104-208 and was made permanent by P.L. 108-447. ARC provides administrative support services on a competitive, fee-for-service, and full-cost basis. ARC's mission is to aid in improving overall government effectiveness by delivering responsive and cost effective administrative support to its Customer Agencies; thereby, improving their ability to effectively discharge their mission.

ARC provides financial management services to approximately 43 customer agencies. Financial management services include accounting, budgeting, reporting, travel and systems support and platform services. The ARC divisions, branches and the financial management services that they provide are:

Accounting Services Division (ASD):

Accounting Operations Branch (AOB)	Document Processing SPS Operations
Accounts and Reports Branch (ARB)	Reporting Services
Accounting Services Branch (ASB)	Document Processing
Treasury Reporting Branch (TRB)	Reporting Services
Funds Management Branch (FMB)	Document Processing Reporting Services
Manufacturing Services Branch (MSB)	Document Processing Reporting Services
Central Accounting Branch (CAB)	Budget Services Supplier Table Update and Maintenance Record and Reconcile Payroll 1099 Reporting

Travel Services Division (TSD):

Temporary Duty Services Branch (TDSB)	Temporary Duty Travel Services Operate/Maintain GovTrip Provide GovTrip Training Services
Relocation Services Branch (RSB)	Relocation Services

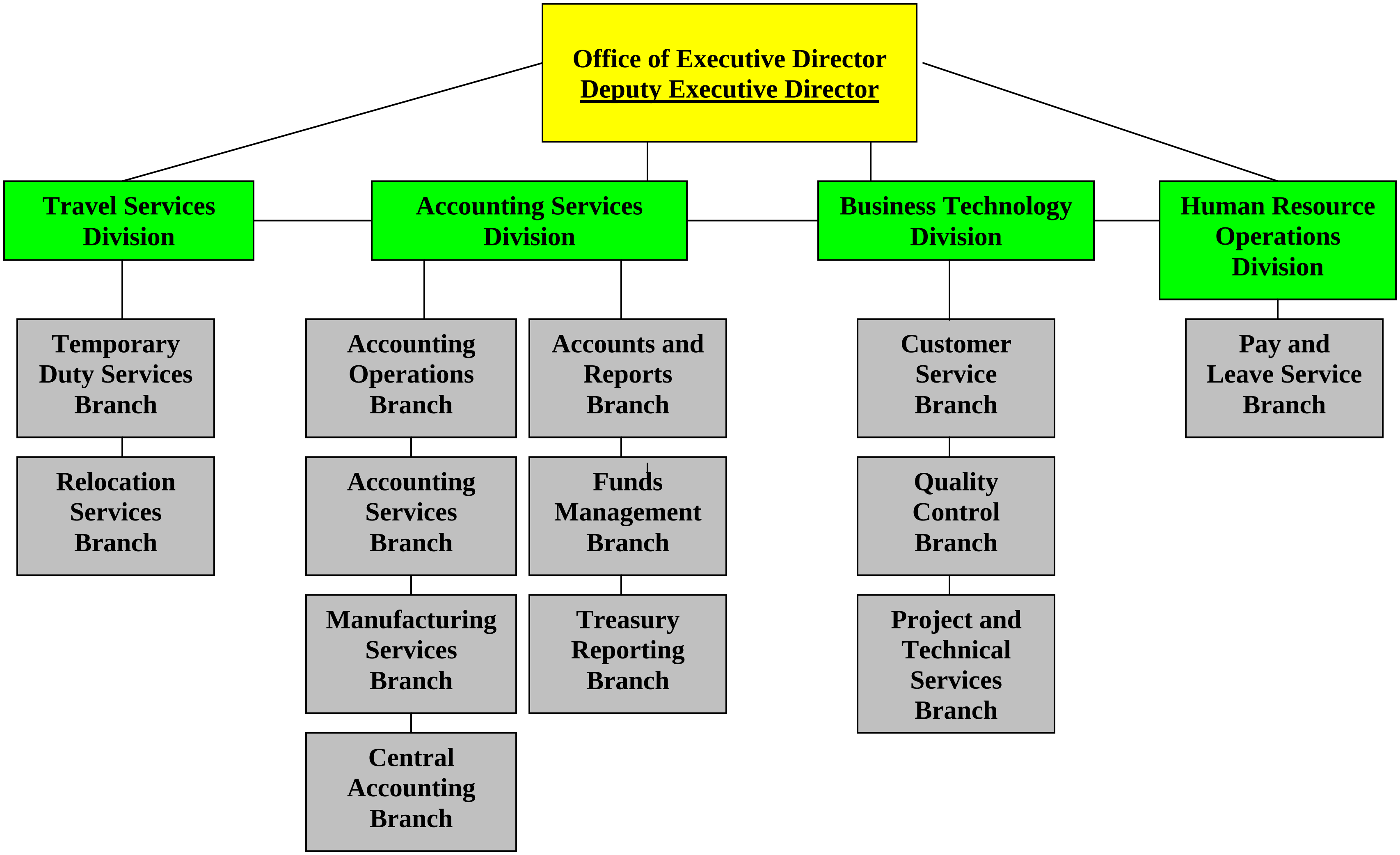
Business Technology Division (BTD)

Customer Service Branch (CSB)	Provide Financial Management System Support/Training
Quality Control Branch (QCB)	Operate/Maintain Financial Management Systems
Project and Technical Services Branch (PTSB)	Application Development/Analysis/Project Management

Human Resources Operations Division (HROD)

Pay and Leave Services Branch (PLSB)	Administer webTA System User Access

ARC Organizational Chart


Office of Executive Director
Deputy Executive Director
Travel Services Division
Accounting Services Division
Business Technology Division
Human Resource Operations Division
Temporary Duty Services Branch
Relocation Services Branch
Accounting Operations Branch
Accounting Services Branch
Manufacturing Services Branch
Central Accounting Branch
Accounts and Reports Branch
Funds Management Branch
Treasury Reporting Branch
Customer Service Branch
Quality Control Branch
Project and Technical Services Branch
Pay and Leave Service Branch

Accounting Services

Accounting Services consists of the following:

- Recording financial transactions in an automated accounting system, including appropriation, apportionment, allocations, revenue agreements, accounts receivable, collections, commitments, obligations, accruals, accounts payable, disbursements, and journal entries.
- Examining and processing vendor and other employee payments.
- Examining and processing revenue and other collections.

To maximize efficiencies and enhance customer satisfaction, ARC has developed financial management service guidelines for Customer Agencies. The guidelines are available to customers via ARC's customer websites. The guidelines provide accounting service overviews, links to regulations and data submission requirements for the various types of services and accounting transactions that ARC processes.

Prior to providing accounting services to Customer Agencies, ARC meets with them to learn and understand the authorizing legislation and mission. This enables ARC to assist them in defining their accounting needs and to ensure that the accounting services provided comply with applicable regulations and are able to meet their internal and external reporting needs.

ARC's automated accounting systems provide for budgeting and funds control at various organizational and spending levels. The levels used are established based on the Customer Agency's authorizing legislation, apportionment level, or their request to control at a lower level than required by law.

ARC offers commitment accounting to Customer Agencies to better enable them to monitor and control their funds availability. When applicable, ARC sets aside funds that are available for obligation based on an approved purchase requisition (PR). In the event that the actual order amount is greater than the approved purchase request amount, a modification to the PR is required unless overage tolerances have been pre-approved by the Customer Agency.

ARC records obligations based on fully executed purchase orders, contracts, training orders or interagency agreements. Recording the obligations in the accounting system sets aside funds to ensure that funds are available to pay for the goods or services when provided and billed by suppliers. All obligations must be approved for funds availability prior to issuance. This is generally done through processing a PR, but is the responsibility of the Customer Agency if they elect not to have commitment accounting services. In the event that the invoice amount is greater than the obligated amount, a modification is required unless overage tolerances have been pre-approved by the Customer Agency.

Customer Agencies are required to notify ARC when goods/services have been received but not invoiced by the supplier at the end of a reporting period. Based on the information received, ARC records expense accruals in the accounting system. The notification process is established at the Customer Agency level and can include submitting receiving reports or schedules that detail the items to be accrued.

ARC processes and/or records all Customer Agency disbursements. These include supplier invoices, purchase card payments, Intra-governmental Payment And Collection (IPAC) transactions, employee travel reimbursements, and employee payroll.

The preferred approach for payment of qualifying supplier goods/services is the government's purchase card program. Customer Agencies are encouraged to obtain and use a government purchase card to the greatest extent possible and they are encouraged to participate in ARC's purchase card program and use Citibank's CitiDirect system. CitiDirect allows Customer Agency cardholders and approving officials to electronically reconcile, route, approve, and submit the purchase card statement to ARC for payment.

Generally, ARC Customer Agencies use two methods of receiving and monitoring the status of supplier invoices. The standard requires that supplier invoices be sent directly to ARC. When using this method, ARC has controls that ensure that all invoices are stamped with the date received, are forwarded to the Customer Agency staff designated on the obligating document for review and approval, and are monitored to ensure that invoices are returned to ARC for processing in accordance with the Prompt Payment Act. The alternative (under unique circumstances) requires that supplier invoices be sent directly to the Customer Agency. When using this method, the Customer Agency is required to establish controls to ensure that all invoices are stamped with the date received, reviewed, certified by the staff member designated on the obligation document, and submitted to ARC for processing in accordance with the Prompt Payment Act.

All invoices are examined by ARC or Customer Agency staff to ensure that they are proper, as defined by the Prompt Payment Act. In addition, invoices are matched to the obligating documents and receiving reports (when applicable) and are certified by contracting officer technical representatives (COTR) or point of contacts (POC). If receiving reports are not submitted, the COTR/POC certifies that the invoice is in accordance with the terms of the order, and provides the dates the goods/services were received and accepted.

After the COTR/POC certifies the invoice, it is submitted to ARC to process the payment to the supplier. The Customer Agency is responsible for ensuring that invoices are submitted in time to receive discounts, if applicable, and to pay the invoice prior to the Prompt Payment Act due date. Upon receipt, ARC reviews the invoice for proper certification, accuracy and completeness and either schedules the payment in accordance with the terms of the order, the Prompt Pay Act and Electronic Funds Transfer (EFT) Rules or returns the invoice to the customer for clarification or additional information.

ARC transmits EFT and check payment files to the US Department of the Treasury using Treasury's Secure Payment System (SPS). In addition, ARC processes most intragovernmental payments using Treasury's IPAC system. ARC obtains Customer Agency approval prior to initiating an IPAC payment to another federal agency. ARC also monitors IPAC activity initiated against the Customer Agency by another federal agency and forwards all IPAC payments to the appropriate certifying official for approval. ARC records all IPAC payments in the accounting period the IPAC was accomplished.

Third-party payroll processors provide ARC with a file of payroll data each week to interface into the accounting system. ARC reconciles all payroll transactions recorded to disbursements reported by the third-party processor. ARC records payroll accruals on a monthly basis and reverses the accrual in the subsequent accounting period. The payroll accrual is a prorated calculation performed by the accounting system that is based on the most recent payroll disbursement data available.

ARC processes revenue and collection related transactions (i.e., unfilled customer orders, receivables, and cash receipts) with Customer Agency approval. Customer Agencies either forward to ARC approved source documents or a summary of their transactions. ARC records IPAC transactions in the period in which they are processed in FMS's IPAC System. Check deposits are made by ARC or the Customer Agency. When checks are deposited by customers, the Standard Form (SF) 215 deposit ticket is forwarded to ARC. In addition, all deposits require the Customer Agencies to provide the accounting information necessary to record the cash receipt.

ARC records proprietary and budgetary accounting entries using the United States Standard General Ledger (USSGL) and Treasury approved budget object codes at the transaction level. In addition, ARC reconciles general ledger accounts to ensure transactions are posted to the appropriate accounts. ARC prepares budgetary to proprietary account relationship reconciliations on a monthly basis to ensure transactions are properly recorded and corrects any invalid out-of-balance relationships.

ARC utilizes FileSurf, a software application managed by BPD's Office of Management Services' (OMS), Information Management Branch (IMB), to store hardcopy data records. ARC generates labels, which are printed and placed on boxes that are to be stored in BPD's warehouse. The information recorded on the label is entered into FileSurf so that the boxes can subsequently be requested by ARC personnel as they are needed. Once the data is recorded in FileSurf, BPD warehouse personnel either pick up the box to be placed in storage or return the box to ARC, as applicable

ARC works with Customer Agencies to develop and implement processes to ensure the accuracy of their accounting information. This includes reviewing open commitment, obligation, expense accrual, customer agreement, and open billing document reports for completeness, accuracy, and validity. This review is conducted by Customer Agencies or ARC staff no less frequently than quarterly. Based on the review, a determination is made on the action(s) needed to adjust or remove any invalid items in ARC's accounting records.

Budget Services

ARC enters the Customer Agency's budget authority in the accounting system based on the supporting documentation, which may include enacted legislation, anticipated resources, Treasury warrants or transfer documents, an Apportionment and Reapportionment Schedule (SF 132), the Customer Agency's budget plan or recorded reimbursable activity. The budget process makes funds available for commitment, obligation, and/or expenditure, and with controls in place, the automated accounting system checks for sufficient funds in the Customer Agency's budget at the specified control levels.

Reporting Services

ARC performs all required external reporting for Customer Agencies, including the following reports: SF 224, FACTS I, FACTS II, Report on Receivables, Treasury Information Executive Repository (TIER), and quarterly and year-end financial statements. In addition, ARC has created a standard suite of management reports that are available to all Customer Agencies. ARC also reconciles certain general ledger accounts and ensures that proprietary and budgetary general ledger account relationships are maintained.

Travel Services

Travel Services consist of the following:

- Operating and maintaining the E-Gov Travel system in compliance with the Federal Travel Regulations (FTR) for all ARC Customer Agencies
- Researching and implementing the FTR and Agency/Bureau travel policies

- System Administration
- Providing customer service and training to system users
- Evaluating, recommending, and implementing approved changes to existing systems and/or new systems, including working with the E-Gov Travel vendor and the General Services Administration (GSA) on system enhancements and deficiencies
- Processing employee reimbursements via interface to ORACLE

Travel documents (authorizations and vouchers) and miscellaneous employee reimbursements are entered by Customer Agencies into GovTrip and are electronically routed to an Approving Official for review and approval. The Approving Official electronically signs the documents with a status of "approved". All "approved" documents are interfaced and reconciled to the core accounting system daily. GovTrip contains system audits that prohibit documents that do not meet certain Federal Travel Regulations or do not contain required accounting information from interfacing to the core accounting system.

Access to GovTrip is restricted to users with a valid logon ID and password. All GovTrip users must complete the self-registration process, which includes being accepted by a TSD Administrator who verifies the request to grant GovTrip access. Budget Reviewers and Approving Officials must complete, sign, and submit a supervisor-approved *Form PD5409E – Administrative Resource Center (ARC) Online Applications Access Request* or have their manager submit an e-mail request to Travel Services. Changes to a user's identification (i.e. name change) require a resubmitted Form PD5409E or an e-mail from the user copying his/her approving official. Changes to a user's role require a resubmitted PD5409E or e-mail approval from the traveler's approving official.

System Platform Services

System Support and Platform Services consist of the following:

- Operating and maintaining the core accounting system, including the feeder interfaces
- Administering user roles
- Providing customer service and training to its system users
- Evaluating, recommending and implementing approved changes to existing systems and/or new systems

ARC has guidelines to ensure authorized and secure access to Customer Agency data. User access to systems is obtained by submitting supervisor-approved *Form PD5409E – Administrative Resource Center (ARC) Online Applications Access Request*. Users specify the system(s) and the level of access required on the form. The user and his/her supervisor must sign the access form. The end user's signature indicates that they are familiar with the Privacy Act information and security requirements and will comply with computer security requirements established by BPD and ARC. The supervisor's signature indicates that the access is authorized. Customer Agency users are also required to maintain up-to-date virus protection software on the computer they use to access ARC applications.

When ARC initially establishes an ORACLE or Prism user account, BTD's CSB e-mails the user requesting that the user call either the ORACLE Support Desk or the Prism Support Desk to receive his/her user ID and temporary password verbally. The appropriate Support Desk provides the User ID and temporary password after verifying the identity of the caller. For internal customers, CSB e-mails the user with a temporary password and reference to their network log in id. Password requirements are provided to the authorized user.

When ARC initially establishes webTA access for a new timekeeper or supervisor, many times the user already has a user ID and password that they have been using to access the employee functionality of the system. If this is the case, HROD's PLSB grants the new level of access and notifies the user via e-mail that they have been given the access. For those agencies whose employees do not input their own time and attendance information, new timekeepers and supervisors must be assigned a user ID and password. In these cases, HROD's PLSB e-mails the user ID and a temporary password. The temporary password provided in the e-mail includes "XXXX," and the user is instructed to replace the "XXXX" with the last four digits of their Social Security Number. Once the user logs on to the system using the temporary password, he/she is prompted to establish a new password.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, AND MONITORING

Control Environment

ARC Financial Management Service operations are primarily under the direction of the Office of the Executive Director of ARC. ARC's mission is to aid in improving overall government effectiveness by delivering responsive and cost effective administrative support to its Customer Agencies; thereby, improving their ability to effectively discharge their mission.

The ASD, BTD, and TSD are responsible for processing and reporting accounting activity and for providing system support, platform, and travel services for Customer Agencies. ARC holds management meetings on a regular basis to discuss special processing requests, operational performance, and the development and maintenance of projects in process. Written position descriptions for employees are maintained. The descriptions are inspected and revised as necessary.

References are sought and background, credit, and security checks are conducted for all BPD personnel when they are hired. Additional background, credit, and security checks are performed every three to five years. The confidentiality of user-organization information is stressed during the new employee orientation program and is emphasized in the personnel manual issued to each employee. BPD provides a mandatory orientation program to all full time employees and encourages employees to attend other formal outside training. Training available to BPD employees with related work responsibilities includes, but is not limited to: Prompt Pay and Voucher Examination, Appropriation Law, Federal Travel Regulations, SF 224 – Statement of Transactions, Dollars & Sense, Standard General Ledger (SGL) Basic, SGL Advanced, SGL Trial Balances and Crosswalks, Budgeting and Accounting – Making the Connection and Computer Security Training Awareness.

All BPD employees receive an annual written performance evaluation and salary review. These reviews are based on goals and objectives that are established and reviewed during meetings between the employee and the employee's supervisor. Completed appraisals are reviewed by senior management and become a permanent part of the employee's personnel file.

Risk Assessment

BPD has placed into operation a risk assessment process to identify and manage risks that could affect ARC's ability to provide reliable accounting and reporting, system platform and travel services for Customer Agencies. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures and controls to manage these risks.

Monitoring

BPD management and supervisory personnel monitor the quality of internal control performance as a normal part of their activities. Management and supervisory personnel inquire of staff and/or review data to ensure that transactions are processed within an effective internal control environment. An example of a key monitoring control is that ASD Reporting Branch Managers and/or Supervisors review reconciliations from the core accounting system subledgers to the related general ledger accounts. ASD prepares budgetary to proprietary account relationship reconciliations on a monthly basis. In addition, ASD prepares and reconciles the FACTS II submitted reports to the trial balance and statement of budgetary resources on a quarterly basis. ARC also uses the results of the annual Statement on Auditing Standards Number 70 (SAS 70) examination as a tool for identifying opportunities to strengthen controls.

INFORMATION AND COMMUNICATION

Information Systems

ORACLE Federal Financials (ORACLE)
ARC operates ORACLE version 11i, with the ORACLE 9i database, which runs on the ARC subnet and accesses data in the ARC Demilitarized Zone (DMZ) using Linux as its operating system. ORACLE uses a two-tier web-based infrastructure with a front-end Internet user interface and a database residing on the secure network. The application (web.net) accesses the database IP to IP on a specified port that is defined in the Access Control List. External Internet access is via a 128-bit Secure Sockets Layer (SSL) encrypted connection. External security is also provided by BPD's Office of Information Technology (OIT) through a PIX firewall and router Access Control Lists. The application is compliant with Section 508 of the Rehabilitation Act Amendment for 1998 for Americans with Disabilities (ADA). ARC also uses a report writer package called Discoverer that provides users with the ability to create their own ad hoc reports for query purposes.

PRISM and GovTrip are feeder systems that interface with ORACLE. webTA feeds data to the National Finance Center (NFC) that is then interfaced with ORACLE. ARC personnel maintain ORACLE, PRISM, and the payroll interface that feeds NFC data to ORACLE. Northrop Grumman Mission Systems (NGMS) developed and hosts GovTrip. OIT serves as the ORACLE database administrator and provides primary support for tape backup and recovery

Functions of the ORACLE accounting system include budget execution, general ledger, purchasing, accounts payable, accounts receivable, fixed assets, and manufacturing.

GovTrip

ARC utilizes NGMS's GovTrip travel system (system selected by the U.S. Department of the Treasury as its E-Gov Travel solution). GovTrip is a web-based, self-service travel system that incorporates traditional reservation and fulfillment support and a fully automated booking process. GovTrip utilizes system processes and audits to ensure compliance to the FTR and/or Agency policy. GovTrip is used to prepare, examine, route, approve, and record travel authorizations and vouchers. It is used to process all temporary duty location (TDY) authorizations, vouchers, local vouchers and miscellaneous employee reimbursements. Approved documents interface to ORACLE for obligation or payment during a scheduled batch process. GovTrip users consist of travelers, document preparers, budget reviewers, and approving officials.

PRISM
ARC uses Compusearch PRISM as its procurement system for Customer Agencies serviced by ORACLE. Transactions entered through PRISM interface real-time with ORACLE.

ARC operates PRISM version 5, with the ORACLE 9i database, which runs on the ARC subnet and accesses data in the ARC DMZ using Windows 2000 as its operating system. OIT serves as the PRISM database administrator and provides primary support for tape backup and recovery. PRISM uses a two-tier web-based infrastructure with a front-end Internet user interface and a database residing on the secure network. The application (web.net) accesses the database on a specified port that is defined in the Access Control List. Only select Internet Protocol (IP) addresses that are defined in the Access Control List are permitted to connect to the database IP.

External Internet access is via a 128-bit SSL encrypted connection. External security is provided by OIT through PIX firewall and router Access Control Lists.

webTA

ARC uses Kronos' webTA as its time and attendance system for most of its Customer Agencies whose payroll is processed by the NFC. Transactions that are entered in webTA interface with NFC, and NFC ultimately sends payroll data back to ARC for an interface into ORACLE.

ARC operates webTA version 3 on Windows 2000. webTA uses the ORACLE 9i database, which runs on the ARC subnet and accesses data in the ARC DMZ using Linux AS 2.1 as its operating system. OIT serves as the webTA database administrator and provides primary support for tape backup and recovery. webTA uses a two-tier web-based infrastructure with a front-end Internet user interface and a database residing on the secure network. The application (web-applet) accesses the database on a specified port that is defined in the Access Control List. Only select IP addresses that are defined in the Access Control List are permitted to connect to the database IP. External Internet access is via 128-bit encrypted connection. External security is provided by OIT through PIX firewall and router Access Control Lists.

Communication

BPD has implemented various methods of communication to ensure that all employees understand their individual roles and responsibilities over processing transactions and controls. These methods include orientation and training programs for newly hired employees, and use of electronic mail messages to communicate time sensitive messages and information. Managers also hold periodic staff meetings as appropriate. Every employee has a written position description that includes the responsibility to communicate significant issues and exceptions to an appropriate higher level within the organization in a timely manner. Managers also make an effort to address continuing education needs of all employees by identifying training opportunities made available through BPD's employee training and career development programs, internal training classes, and professional conferences.

CUSTOMER AGENCY CONTROL CONSIDERATIONS

BPD's accounting processing and general computer controls related to ARC’s financial management services were designed with the expectation that certain internal controls would be implemented by Customer Agencies. The application of such controls by the Customer Agencies is necessary to achieve all control objectives identified in this report, since ARC is a servicing organization that processes transactions that directly affect Customer Agencies.

This section describes certain controls that Customer Agencies should consider for achievement of control objectives identified in this report. The Customer Agency control considerations presented below should not be regarded as a comprehensive list of all controls that should be employed by Customer Agencies. Customer Agencies should establish controls to:

- Properly approve and accurately enter obligations into the procurement and travel systems in the proper period.

- Send valid requests to record manual obligations to ARC in a timely manner.

- Review open obligation reports for completeness, accuracy, and validity.

- Restrict Customer Agency access to ORACLE, Discoverer, PRISM, webTA, and GovTrip to authorized individuals.

- Communicate Customer Agency required levels of budget and spending controls to ARC.

- Compare actual spending results to budgeted amounts.

- Review the financial reports provided by ARC to ensure that disbursement transactions are complete and accurate.

- Provide certification of *FACTS II to ARC* prior to ARC’s FACTS II system certification.

- Approve invoices for payment and send approved invoices to ARC in a timely manner.

- Ensure that invoices properly reflect the invoice receipt date and formal acceptance date according to the Prompt Payment Act.

- Approve travel vouchers and accurately enter the vouchers into GovTrip in the proper period.

- Maintain and communicate to ARC, a list of individuals authorized to approve invoices and travel vouchers when it is not communicated in the authorizing agreement.

- Send approved and accurate documentation of unfilled customer orders, receivables, cash receipts, advances, and write-off transactions to ARC in the proper period.

- Review unfilled customer orders, receivable and advance reports for completeness, accuracy, and validity.

- Monitor and pursue collection of delinquent balances.

- Review the financial reports provided by ARC to ensure that payroll accruals are complete and accurate.

- Verify that payroll processed by third-party providers is complete and accurate.

- Review the financial reports provided by ARC to ensure that payroll disbursements are complete and accurate.

- Review open accrual reports for completeness, accuracy, and validity.

- Approve and send revenue and expense accruals to ARC in a timely manner.

- Review the financial reports prepared by ARC to ensure that all reports prepared for external use are complete, accurate, and submitted in a timely manner.

- Review the financial reports provided by ARC to ensure that budget entries are complete and accurate.

- Send approved budget plans to ARC in a timely manner.

- Review and approve listing of users with current ORACLE, Discoverer, PRISM, webTA, and GovTrip access to ensure appropriateness.

- Ensure exiting employee timecards are coded “Final” as this will help ensure that HR staff deactivate the employee’s webTA access.

- Send valid requests to record manual journal entries to ARC in a timely manner.

- Maintain and communicate to ARC, a list of individuals authorized to submit manual journal entries that are initiated by the Customer Agency.

- Communicate OMB apportionment status to ARC.

- Monitor usage of budget authority during periods of operation under a Continuing Resolution to ensure that OMB directed apportionment limits are not exceeded.

Specific Customer Agency control considerations are provided for Control Objectives 1, 2, 3, 5, 6, 8, 9, 10, 11, 12 and 13 in the Control Objectives, Related Controls, and Tests of Operating Effectiveness section of this report.

SUB-SERVICE ORGANIZATIONS

In order to provide financial management services, ARC relies on systems and services provided by other organizations external to BPD (sub-service organizations). The following describes the sub-service organizations used by ARC that are included in this report. KPMG LLP's examination did not extend to controls of these sub-service organizations and associated systems.

Name of Sub-service Organization	Name of System	Function/Responsibilities
Treasury Financial Management Service (FMS)	Government Wide Accounting (GWA) Account Statement	Treasury's FMS provides reports to inform agencies of their Fund Balance With Treasury and to assist agencies in reconciling their general ledger balances to FMS balances. ARC uses these reports for the performance of reconciliations.
	Secure Payment System (SPS)	ARC uses SPS to process payments for invoices.
	CA$HLINK II, Regional Finance Center (RFC) Agency Link, Intragovernmental Payment and Collection transactions (IPACs)	Each month, Treasury's FMS issues the FMS 6652, *Statement of Differences*, to agency location codes (ALC) when differences are identified between the cash activity reported by the agency on the SF 224, *Statement of Transaction*s, and data reported to Treasury's CA$HLINK II, RFC Agency Link, and IPAC systems. ARC accountants minimize month-end disbursement differences by comparing preliminary SF 224 data to data obtained from Treasury's CA$HLINK II, RFC Agency Link, and IPAC systems.
Treasury Financial Management Service (FMS)	FACTS I	Treasury's FMS maintains the FACTS I system. The FACTS I system has edit checks to verify that the submitted USSGL accounts and attributes are valid and have equal debit and credit balances.

Name of Sub-service Organization	Name of System	Function/Responsibilities
	FACTS II	Treasury's FMS maintains the FACTS II system. The FACTS II system performs USSGL edit checks and rejects any files that fail the edit checks.
Treasury	Treasury Information Executive Repository (TIER)	For ARC's Treasury and the Department of Homeland Security Customer Agencies, FACTS I and II reporting requirements are met using TIER. TIER is Treasury's departmental data warehouse that receives monthly uploaded financial accounting and budgetary data from the Treasury bureaus and other reporting entities within the Department of the Treasury in a standardized format. Data submitted to TIER by an ARC accountant is validated based on system-defined validation checks. ARC has customized programs in its core accounting system that extract the accounting and budgetary data in the required TIER format. TIER has a standardized chart of accounts that is compliant with USSGL guidance issued by the Department of the Treasury. FACTS II edit checks are incorporated in the TIER validation checks. After submitting the adjusted trial balances into TIER, ARC accountants review the edit reports and resolve any invalid attributes or out-of-balance conditions. ARC accountants document this review by completing the TIER Submission Checklist, which is further reviewed by a supervisor.
	Financial Analysis and Reporting System (FARS)	Treasury's FARS produces financial statements using data bureaus have submitted to TIER.

Name of Sub-service Organization	Name of System	Function/Responsibilities
Various third-party payroll processors	Various systems	Third-party payroll processors transmit payroll files to ARC during the second week after the end of a pay period. ARC uses these files for processing payroll disbursements.
Northrop Grumman Mission Systems (NGMS)	GovTrip	NGMS developed and hosts the GovTrip system, which is an E-Gov travel platform. NGMS is the vendor for E-Gov travel selected by the Department of the Treasury. NGMS maintains the data in their Business Data Warehouse for six years and three months.

III. CONTROL OBJECTIVES, RELATED CONTROLS, AND TESTS OF OPERATING EFFECTIVENESS

ACCOUNTING PROCESSING CONTROLS

Control Objective 1 - Obligations

Controls provide reasonable assurance that obligations are authorized, reviewed, documented, and processed timely in accordance with Administrative Resource Center (ARC) policies and procedures.

Description of Controls

ARC has documented procedures for staff to follow for the processing of obligations.

<u>PRISM System Interface</u>
An obligation is created when a Customer Agency enters into a legally binding contract with a vendor for goods or services. The obligation is entered into ARC's core accounting system through an interface between PRISM and ORACLE Federal Financials (ORACLE). The interface changes the budget status from a commitment (if applicable) to an obligation in the general ledger and updates the corresponding system tables. The interface between the procurement and accounting systems is real-time. The procurement system has built-in controls that validate information provided by the Customer Agency and ensure proper authorization is granted prior to the interface into the accounting system. These include:

- Limited options based on roles;
- Field inputs limited to look-up tables;
- Editable fields are validated;
- Pre-populated fields for default or standard entries;
- Validation of fund availability; and
- Non-editable fields (i.e., total when amount is per unit).

The interface between PRISM and ORACLE is reviewed on a daily basis by a systems analyst. The analyst reviews a report that identifies transactions that have been in the Pending Financial Approval status for more than 15 minutes and transactions that were disapproved during the Pending Financial Approval status. Additionally, for transactions that terminate in Pending Financial Approval status, the report indicates that when ORACLE attempted to insert the record into the general ledger database a successful message was not returned. The report lists all transactions currently in this state. The analyst investigates all transactions included in the report to resolve the issues and change the status accordingly. Additionally, the Customer Agency approver receives notification of the failure in their PRISM inbox if the document status is disapproved.

<u>Manually Recorded Obligations – Customer Agency Approval</u>
For obligations not processed through the interface, Customer Agencies and/or Procurement send ARC a properly signed hardcopy of the agreement, or send ARC an e-mail to obligate the funds. Upon receipt from the Customer Agency, the ARC technician responsible for processing the Customer Agency's accounting transactions reviews the documentation to ensure that adequate accounting information has been received, and manually enters the obligation into ORACLE. Obligations that are posted in ORACLE are available for both ARC and Customer Agency review through ad hoc Discoverer reports.

Travel System Interface

Customer Agencies enter travel authorizations into GovTrip and electronically route them to Approving Officials for review and approval. Approving Officials electronically sign the authorization with a status of “approved”. All “approved” authorizations are interfaced daily via batch processing to the core accounting system which records an obligation in the general ledger. Each day an interface file is received from Northrop Grumman Mission Systems (NGMS) which is used for processing, report generation, and identification of exceptions. The file is loaded into the ORACLE interface and accepted records are added to the core accounting system as obligations in the general ledger. A Status Order exception report is generated and reviewed to identify and correct data interface errors and exceptions between GovTrip and ORACLE. To correct transactions of this nature, the transactions are manually entered into the system. Approved authorizations in GovTrip are reconciled daily by an accounting technician with an ORACLE generated report to ensure that all GovTrip authorizations have been interfaced and processed in ORACLE.

Budget Execution System Controls

Customer Agencies can establish and monitor both legally established and internally developed budget plans in ORACLE to ensure obligations are properly authorized and recorded. Budget plans can be established at the following levels of the accounting structure in ORACLE:

- Appropriation/Fund (Based upon the customer’s appropriation)
- Apportionment (Based upon the apportionment schedule on the Standard Form SF32)
- Cost Center (Based upon the customer’s internal budget plan)
- Reporting Category (Based upon the customer’s internal budget plan)
- Project Code (Based upon the customer’s internal budget plan)
- Budget Object Code (Based upon the customer’s internal budget plan)

Budget execution system controls can be set to prevent spending beyond the budget plan amount or allow spending over the budget plan amount at any level of the budget plan. Spending beyond the apportionment and appropriation levels (legal levels) are prohibited. Decisions on control settings that permit or prevent spending beyond other budget plan levels are made by the Customer Agency. System controls are applied at the fund level after passage of appropriation legislation until a customer agency provides an appropriate financial plan. Upon receipt and input of the budget plan, controls will be established at the detail level dictated by the Customer Agency.

Budget execution settings are determined by the Customer Agency and input into ORACLE by the Customer Service Branch (CSB). System settings are reviewed with the Customer Agency on an annual basis. Budget plans are input into ORACLE by ARC staff, based upon budget plans provided by Customer Agencies.

Document Numbering

All accounting entries recorded in ARC’s core accounting system require a transaction or document identification number. System controls prohibit the use of duplicate document numbers on obligating documents. ARC has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of ARC reports to better identify and/or determine the nature of transactions processed by ARC. When an ARC user attempts to enter a transaction identification number that already exists, the accounting system issues an error message that alerts the user of the duplication.

Customer Agency Control Considerations

Customer Agencies should establish controls to:

- Properly approve and accurately enter obligations into the procurement and travel systems in the proper period.

- Send valid requests to record manual obligations to ARC in a timely manner.

- Review open obligation reports for completeness, accuracy, and validity.

- Restrict Customer Agency access to ORACLE, Discoverer, PRISM, webTA, and GovTrip to authorized individuals.

- Communicate Customer Agency required levels of budget and spending controls to ARC.

- Compare actual spending results to budgeted amounts.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for the processing of obligations and observed ARC staff process obligations, and determined that transactions were processed in accordance with the procedures.

- Observed built-in validation PRISM checks reject invalid transactions and noted that validation controls were functioning.

- Inspected a selection of Discoverer reports showing the cumulative PRISM to ORACLE interface errors and determined that the reports were reviewed to identify and correct data interface errors and exceptions between PRISM and ORACLE.

- For a selection of obligations interfaced through feeder systems, inspected the related general ledger entries, and corresponding contracts and travel vouchers and determined that the obligations were processed timely.

- For a selection of manually entered obligations, inspected the related general ledger entries, and corresponding contracts and travel vouchers and determined that the obligations were authorized and were processed timely.

- Observed an ARC staff member enter travel vouchers into GovTrip and noted that the system required the travel vouchers to be routed to an approving official.

- Observed an approving official attempt to enter and approve travel vouchers and noted that GovTrip prevented a user from both entering and approving travel vouchers.

- For a selection of dates, inspected GovTrip to ORACLE exceptions reports and determine that reports were reviewed to identify and correct data interface errors or exceptions between GovTrip and ORACLE.

- For a selection of budget execution settings that were input during the review period, inspected evidence of Customer Agency review and the instructions from the Customer Agency, and compared them to the Discoverer reports detailing the budget settings. Determined that the budget execution settings input by ARC were reviewed and authorized by the Customer Agency.

- Observed ARC staff attempt to enter a budget transaction into ORACLE in excess of a budget limit and noted that the system prevented the entry.

- Observed an ARC staff member attempt to enter a transaction into ORACLE with a document number that had already been entered into ORACLE and noted that ORACLE automatically rejected the entry of a duplicate document number.

No exceptions noted.

Control Objective 2 - Disbursements

Controls provide reasonable assurance that the disbursement of invoices and vouchers is authorized, reviewed, processed timely, reconciled, and properly documented in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures for staff to follow for the processing of disbursements.

Customer Agency Invoice Approvals
ARC only processes disbursements for invoices with Customer Agency approval. Vendors can either send invoices to the Customer Agency or ARC, depending on the instructions in the purchase order. If invoices are sent to the Customer Agency, the Customer Agency reviews and approves the invoice and forwards the invoice and documentation of Customer Agency approval to ARC. If invoices are sent to ARC, ARC either faxes or digitally scans and e-mails the invoice to the authorized Customer Agency contact for approval. Appropriate contacts are either specified in the purchase order or are communicated to ARC by the Customer Agency. Intragovernmental Payment and Collection transactions (IPACs) which decrease an ARC Customer Agency's Fund Balance with Treasury (FBWT) must be approved in advance by the Customer Agency, unless the IPAC was initiated against the Customer Agency by another federal agency. To ensure that IPAC transactions initiated against the Customer Agency by another federal agency are posted in the proper accounting period, ARC may obtain Customer Agency approval after the IPAC has been recorded. Disbursement may also occur with information from feeder systems (PRISM and GovTrip.)

Statistical Sampling of Invoices
All invoices are subject to ARC internal review. System controls set at the user identification and/or vendor level ensure that payment of invoices greater than $2,500 which are processed by an accounting technician must be reviewed and approved by a lead accounting technician or an accountant. Invoices less than $2,500 are subject to statistical sampling by a lead accounting technician or an accountant. System user access profiles restrict accounting technicians' ability to process documents that require secondary review and approval and ensure proper segregation of duties is maintained. A 100% post audit management review is conducted monthly on all invoices greater than $2,500 that are both processed and approved by the same individual.

Travel Voucher Reconciliations
Customer Agencies enter travel vouchers into GovTrip and electronically route them to Approving Officials for review and approval. Approving Officials electronically sign the voucher with a status of "approved". All "approved" travel vouchers are interfaced daily via batch processing to the core accounting system which records a disbursement in the general ledger. Each day an interface file is received from Northrop Grumman which is used for processing, report generation, and identification of exceptions. The file is loaded into the ORACLE interface and accepted records are added to the core accounting system as disbursements in the general ledger. The travel voucher is then matched against an existing authorization. A Status Voucher report is generated and reviewed to identify and correct data interface errors and exceptions between GovTrip and ORACLE. To correct transactions of this nature, the transactions are manually entered into the system. Approved vouchers in GovTrip are reconciled daily by an accounting technician with an ORACLE generated report to ensure that all GovTrip vouchers have been interfaced and processed in ORACLE.

Statistical Sampling of Travel Vouchers

An accounting technician or junior analyst completes a post audit review of travel vouchers to verify the accuracy of the interfaced data and compliance with Federal Travel Regulations (FTR), using statistical sampling procedures to select documents less than $2,500, based on the Customer Agency's travel policy (FTR or FTR/ARC). A 100% post audit review is conducted on all documents greater than $2,500. Errors discovered during the review are sent via e-mail to the traveler or document preparer and approving official to review and/or take action. Billing documents are created for amounts owed by a traveler of $25 or greater, resulting from an overpayment. The traveler sends a check to cover the overpayment.

Payment Date Calculations

Based on the Customer Agency's contracts with its suppliers, ARC staff enters the invoice date and the later of the invoice receipt date, or the earlier of the formal or constructive acceptance dates into ORACLE based on the supporting documentation from the Customer Agency. On a daily basis, ORACLE selects invoices that are due for payment and creates files for manual uploading into Treasury's Secure Payment System (SPS). The ARC SPS certifying officer compares the number and dollar amount of payments from the SPS generated schedule to the payment files generated by ORACLE to ensure all payment files have been uploaded to Treasury. The ARC SPS certifying officer also confirms that the routing and account number supplied in the payment file being uploaded to Treasury agrees with the banking information in the accounting system. For invoices that are subject to the Prompt Payment Act, ORACLE schedules payments to disburse 30 days after the later of the invoice receipt date and the earlier of the date of formal or constructive acceptance (unless the supplier's contract or invoice states otherwise). Any payments that are subject to the Prompt Payment Act that are paid after their ORACLE scheduled due date are subject to prompt pay interest to cover the period the payment was due but not paid. ORACLE automatically determines if interest is due based on the dates in the accounting system. If interest is due, ORACLE calculates interest and generates an interest payment to the vendor, provided the total interest is more than one dollar**.**

Reconciliation – Fund Balance With Treasury Activity

Each month, Treasury's Financial Management Service (FMS) issues the *Statement of Differences* to agency location codes (ALC) when differences are identified between the cash activity reported by the agency on the SF 224, *Statement of Transactions*, and data reported to Treasury's CA$HLINK II, Regional Finance Center (RFC) Agency Link, and IPAC systems. ARC accountants minimize month-end disbursement differences by comparing preliminary SF 224 disbursement data to data obtained from Treasury's CA$HLINK II, RFC Agency Link, and IPAC systems. Any differences identified by the accountant are corrected by an accounting technician or another accountant prior to the close of the accounting period. ARC accountants prepare monthly *Statement of Differences* reconciliations for supervisory review. If a *Statement of Differences* was received, the transaction(s) that caused the difference is (are) identified and if necessary correcting entries are posted by an accounting technician or another accountant and reported in the subsequent accounting period.

Budget Execution System Controls

Customer Agencies can establish and monitor both legally established and internally developed budget plans in ORACLE to ensure obligations are properly authorized and recorded. Budget plans can be established at the following levels of the accounting structure in ORACLE:

- Appropriation/Fund (Based upon the customer's appropriation)
- Apportionment (Based upon the apportionment schedule on the SF132)
- Cost Center (Based upon the customer's internal budget plan)

- Reporting Category (Based upon the customer's internal budget plan)
- Project Code (Based upon the customer's internal budget plan)
- Budget Object Code (Based upon the customer's internal budget plan)

Budget execution system controls can be set to prevent spending beyond the budget plan amount or allow spending over the budget plan amount at any level of the budget plan. Spending beyond the apportionment and appropriation levels (legal levels) are prohibited. Decisions on control settings that permit or prevent spending beyond other budget plan levels are made by the Customer Agency. System controls are applied at the fund level after passage of appropriation legislation until a customer agency provides an appropriate financial plan. Upon receipt and input of the budget plan, controls will be established at the detail level dictated by the Customer Agency.

Budget execution settings are determined by the Customer Agency and input into ORACLE by the CSB. System settings are reviewed with the Customer Agency on an annual basis. Budget plans are input into ORACLE by ARC staff, based upon budget plans provided by Customer Agencies.

<u>Document Numbering</u>
All accounting entries recorded in ARC's core accounting system require a transaction or document identification number. System controls in ORACLE prohibit the use of duplicate document numbers for the same vendor on accounts payable transactions. ARC has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of ARC reports to better identify and/or determine the nature of transactions processed by ARC. When an ARC user attempts to enter a transaction identification number that already exists, the accounting system issues an error message that alerts the user of the duplication.

Customer Agency Control Considerations

Customer Agencies should establish controls to:

- Review the financial reports provided by ARC to ensure that disbursement transactions are complete and accurate.

- Approve invoices for payment and send approved invoices to ARC in a timely manner.

- Ensure that invoices properly reflect the invoice receipt date and formal acceptance date according to the Prompt Payment Act.

- Approve travel vouchers and accurately enter the vouchers into GovTrip in the proper period.

- Maintain and communicate to ARC, a list of individuals authorized to approve invoices and travel vouchers when it is not communicated in the authorizing agreement.

- Communicate Customer Agency required levels of budget and spending controls to ARC.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for the processing of disbursements and observed ARC staff process disbursements, and determined that the transactions were processed in accordance with the procedures.

- For a selection of disbursements, inspected documentation of Customer Agency authorization and related general ledger entries and determined that disbursements were authorized and processed timely.

- Observed an ARC accounting technician attempt to process and approve an invoice larger than $2,500 and noted that the technician was unable to approve the invoice, and that the transaction required secondary approval from an ARC accountant or lead accounting technician for processing.

- For a selection of months, inspected post-audit management reviews of all invoices greater than $2,500 that were both processed and approved by the same individual and determined that post-audit management reviews were conducted by the individual's supervisor.

- Observed an ARC staff member enter travel vouchers into GovTrip and noted that the system required the travel vouchers to be routed to an approving official.

- Observed an approving official attempt to enter and approve travel vouchers and noted that GovTrip prevented a user from both entering and approving travel vouchers.

- For a selection of dates, inspected GovTrip to ORACLE interface reconciliations, and determined that daily reconciliations were performed to determine if approved GovTrip vouchers were interfaced and processed in ORACLE, and to identify and correct data interface errors and exceptions between GovTrip and ORACLE.

- For a selection of months, inspected post audit travel voucher reviews and determined that reconciliations were performed and any exceptions were resolved.

- Inspected a selected invoice record due for payment in ORACLE, and compared the date that it became due for payment to the date that ORACLE automatically added a related disbursement to the SPS data file and determined that disbursements were timely initiated by ORACLE.

- For a selection of dates, inspected SPS certifying officer reports and determined that reports comparing the SPS generated schedule to the payment files generated by ORACLE were reviewed and that any exceptions were resolved.

- For a selection of months, inspected SF 224 reconciliations and determined that reconciliations were documented and that any exceptions were resolved.

- For a selection of months, inspected FMS 6652 (*Statement of Difference*) reconciliations and determined that reconciliations were documented and that any exceptions were resolved.

- For a selection of budget execution settings that were input during the review period, inspected evidence of Customer Agency review and the instructions from the Customer Agency, and compared them to the Discoverer reports detailing the budget settings. Determined that the budget execution settings input by ARC were reviewed and authorized by the Customer Agency.

- Observed ARC staff attempt to enter a budget transaction into ORACLE in excess of a budget limit and noted that the system prevented the entry.

- Observed an ARC staff member attempt to enter a transaction into ORACLE with a document number that had already been entered into ORACLE and determined that ORACLE automatically rejected the entry of a duplicate document number.

- Inspected a selected invoice that was paid late and determined that the system-calculated Prompt Pay interest was mathematically accurate.

No exceptions noted.

Control Objective 3 – Unfilled Customer Orders, Receivables, and Cash Receipts

Controls provide reasonable assurance that unfilled customer orders, receivables, and cash receipts are reconciled and properly documented in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures for staff to follow for the processing of unfilled customer orders, receivables, and cash receipts.

Customer Agency Approval
ARC only processes unfilled customer orders, receivables, and cash receipts with Customer Agency approval, with the exception of checks received for deposit directly by ARC on the customer's behalf for accounts payable invoice refunds of overpayments and/or vendor rebates. Customer Agencies either send properly signed source documents or provide a summary of their transactions via fax or e-mail. ARC enters all transactions into ORACLE which are available for review through reporting systems. To help ensure that cash receipts are posted in the proper accounting period, ARC may obtain Customer Agency approval after the cash receipt has been recorded.

Reconciliation – Fund Balance With Treasury Activity
Each month, Treasury's FMS issues the *Statement of Differences* to ALCs when differences are identified between the cash activity reported by the agency on the SF 224, *Statement of Transactions*, and data reported to Treasury's CA$HLINK II and IPAC systems. ARC accountants minimize month-end differences relating to collections by comparing preliminary SF 224 collection data to Treasury's CA$HLINK II and IPAC systems. Any differences identified by the accountant are corrected by an accounting technician or another accountant prior to the close of the accounting period. ARC accountants prepare monthly *Statement of Differences* reconciliations for supervisory review. If a *Statement of Differences* was received, the transaction(s) that caused the difference is (are) identified and correcting entries are posted by an accounting technician or another accountant and reported in the subsequent accounting period.

Reporting - Receivables
ARC accountants prepare and submit a quarterly *Report on Receivables Due from the Public* for all Customer Agencies. This report requires agencies to track the collection of receivables and report on the status of delinquent balances according to an aging schedule. Accountants that are responsible for preparing the *Report on Receivables Due from the Public* review and reconcile all activity (i.e., new receivables, revenue accruals, collections, adjustments and write-offs) with the public on a quarterly basis. An ARC supervisory accountant reviews the report. Customer Agencies are responsible for monitoring and pursuing collection of delinquent balances. On an annual basis, the Customer Agency's Chief Financial Officer must certify that the report submitted to the Department of the Treasury is accurate and consistent with agency accounting systems.

Intragovernmental Transactions
ARC adheres to applicable intragovernmental elimination guidance. This involves recording transactions at a level that allows for identification of its governmental trading partners and for reconciling the transactions/balances with trading partners on a quarterly basis. For its non-Treasury and non-Homeland Security Customer Agencies, ARC accountants reconcile fiduciary account balances with their trading partners (Bureau of Public Debt, Office of Personnel

Management and Department of Labor) after uploading account balances into the Intragovernmental Fiduciary Confirmation System (IFCS). The Department of Treasury and the Department of Homeland Security utilize IFCS to reconcile Treasury and Homeland Security agency fiduciary account balances with trading partners. For the non-fiduciary transactions of its Customer Agencies, ARC accountants prepare and submit confirmations to the appropriate trading partners in accordance with the elimination reconciliation guidance. Upon submitting the confirmations to the trading partners, ARC works with the trading partners to reconcile transactions/balances and identify and record any necessary adjustments. Reconciliations are not performed for non-Treasury customer agencies. Non-Treasury customer agencies receive confirmations only.

Document Numbering
All accounting entries recorded in the core accounting system require a transaction or document identification number. System controls prohibit the use of duplicate document numbers on unfilled customer orders and receivables. A system control alerts the user of the use of duplicate document numbers on cash receipt and advance transactions. ARC has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of ARC reports to better identify and/or determine the nature of transactions processed by ARC. When an ARC user attempts to enter a transaction identification number that already exists, the accounting system issues an error message that alerts the user of the duplication.

Customer Agency Control Consideration

Customer Agencies should establish controls to:

- Send approved and accurate documentation of unfilled customer orders, receivables, cash receipts advances, and write-off transactions to ARC in the proper period.

- Review unfilled customer orders, receivable and advance reports for completeness, accuracy, and validity.

- Monitor and pursue collection of delinquent balances.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for the processing of unfilled customer orders, receivables, and cash receipts and observed ARC personnel process transactions, and determined that the transactions were processed in accordance with the procedures.

- For a selection of unfilled customer orders, receivables and cash receipts, inspected documentation of Customer Agency authorization and determined that transactions were authorized by Customer Agencies.

- For a selection of months, inspected SF 224 reconciliations and determined that reconciliations were documented and that any exceptions were resolved.

- For a selection of months, inspected FMS 6652 (*Statement of Difference*) reconciliations and determined that reconciliations were documented and that any exceptions were resolved.

- For a selection of quarters, inspected *Report on Receivables Due from the Public* reconciliations and determined that reconciliations were documented and that any exceptions were resolved.

- For a selection of quarters, inspected *Reports on Receivables Due from the Public* and determined that they were reviewed by an ARC supervisory accountant.

- Inspected a selection of intra-governmental confirmations and reconciliations and determined that confirmations were sent and that reconciliations were documented, and exceptions were resolved

- Observed an ARC staff member attempt to enter a transaction into ORACLE with a document number that had already been entered into ORACLE and determined that ORACLE automatically rejected the entry of a duplicate document number.

No exceptions noted.

Control Objective 4 - Deposits

Controls provide reasonable assurance that checks are secure and deposited timely by appropriate personnel and documented in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures for the safeguarding and recording of deposits.

Manual Deposits – Segregation of Duties

Checks received by the mailroom are scanned and a batch ticket with the number of checks received is generated. Copies of the batch ticket along with the checks are sent via confidential mail to the appropriate ARC branch. An ARC branch secretary or Office Automation Assistant who does not have accounting system access to post account receivable transactions, receives, opens and logs all checks received in the branch's check deposit log. The number of checks received is compared to the number of checks listed on the batch ticket. Checks are to be deposited as soon as possible after the purpose and validity of the check's issuance are identified. While the accounting technician responsible for processing deposits for the Customer Agency is researching the check's purpose and validity, the check is locked in a secretary's drawer until it is ready to be deposited. When the check is ready for deposit, a deposit ticket and the check are placed in a locked bag and picked up by the mail clerk. A copy of the deposit ticket is retained by the branch secretary for comparison with the receipt and deposit ticket signed by the bank teller. The mail clerk delivers the locked bag containing the deposit ticket and checks to the local federal depository. The bag containing the bank teller's deposit ticket and receipt are returned to the branch office that processed the deposit. After the bank teller receipt and deposit ticket are compared to the copy retained by the branch and the secretary updates the check deposit log to record the date the deposit was made, an accounting technician processes the cash receipt in the accounting system.

Paper Check Conversion System Deposits and Reconciliation

For customers using the Paper Check Conversion (PCC) system, the management assistant hand delivers all checks received and logged prior to noon, along with the checks received after noon of the previous business day, to the ARC technician. The ARC technician or secretary scan each check into the PCC system. The batch list is automatically temporarily saved to the server until it is transmitted to the Federal Reserve Bank (FRB) by the technician. Upon settlement with the FRB, the ARC technician reconciles the batch list with the paper checks and signs off indicating the reconciliation is complete. After reconciliation, the checks are stamped "VOID" by the management assistant and held awaiting confirmation of the deposit in CA$HLINK II. Upon confirmation in CA$HLINK II, the ARC technician is notified by the management assistant to destroy the checks. The cash receipt is recorded in ORACLE by the ARC technician and reviewed and approved by an accountant.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for the safeguarding and recording of deposits and observed ARC staff process checks, and determined that checks were processed in accordance with the procedures.

- Inspected the check deposit logs and a list of users with access to post collections in ORACLE. Determined that the logging of checks was performed by individuals without access to post collections in ORACLE.

- For a selection of dates, inspected batch tickets generated by the mail room upon check receipt and the corresponding check log. Determined that the batch tickets were created and that checks were accurately reported on the check log.

- For a selection of un-deposited checks from the check deposit log, inspected the checks and determined that they were properly secured in a locked drawer.

- Inspected a selection of signed check deposit logs and determined that the checks were deposited timely and documented.

- Inspected a selection of reconciliations from the deposit tickets to the bank teller deposit tickets and receipts and determined that the reconciliations were performed.

- For a selection of dates, inspected PCC reconciliations and determined that the reconciliations were performed and that any exceptions were resolved.

- For a selection of dates, inspected batch tickets generated by the mail room upon check receipt and the corresponding check log. Determined that the batch tickets were created and that checks were accurately reported on the check log.

No exceptions noted.

Control Objective 5 – Payroll Accruals

Controls provide reasonable assurance that period-end payroll accruals are processed timely, reviewed, and properly documented in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures for staff to follow for the processing of payroll accruals.

System Calculation of Accruals
Payroll accruals are recorded on a monthly basis and reversed in the subsequent accounting period. The payroll accrual is a prorated calculation performed by the accounting system that is based on the most recent payroll disbursement data available. To make its calculation, the accounting system requires a payroll accountant to enter specific parameters (e.g., number or percentage of workdays to accrue and the base pay period number).

Manual Verification of Accruals
A payroll accountant independently reviews the accounting system calculated accrual for reasonableness. The payroll accountant recalculates the accrual using an Excel spreadsheet to multiply the last full pay period disbursement by the number of days accrued divided by ten days. The payroll accountant compares the recalculated payroll amount to the accounting system calculation for reasonableness. The payroll accountant researches and identifies any material differences not explained by non-recurring budget object classes. Those differences are corrected in the period in which they are identified. The payroll accountant provides the spreadsheet to a supervisor or manager for review and approval.

Customer Agency Control Considerations

- Review the financial reports provided by ARC to ensure that payroll accruals are complete and accurate.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for the processing of payroll accruals and observed ARC staff process payroll accruals, and determined that the processing was in accordance with the procedures.

- For a selection of months, inspected supervisor signed payroll verification spreadsheets and payroll accrual invoices for entry into ORACLE and determined that payroll accruals were verified and entered timely.

- For a selection of months, inspected payroll accrual invoices for entry into ORACLE and determined that payroll accruals were entered timely.

No exceptions noted.

Control Objective 6 – Payroll Disbursements

Controls provide reasonable assurance that payroll disbursement data (disbursed by a third-party) is reviewed, reconciled, and properly documented in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures for staff to follow for the processing of payroll disbursements.

Automated Payroll Posting Process

Third-party payroll processors transmit payroll files to ARC during the second week after the end of a pay period. Upon converting the data into a format that can be uploaded into the ORACLE accounting system, the ARC payroll accountant reconciles the converted data to the original raw data from the third-party processors. The ARC payroll accountant processes payroll entries using a batch interface that posts summary payroll data to the core accounting system. The payroll accountant reviews and corrects transactions that reject in the interface. A Discoverer report is used to identify those records that reject. The payroll accountant contacts the customer for resolution of erroneous accounting codes, funding issues, or other circumstances that would prevent the payroll from being recorded. Until the errors are cleared, the data are viewed as invalid and will not be able to be transferred to the core accounting system. If the third-party payroll processor provides adjustment files for additional transactions between main payroll files, the ARC payroll accountant follows the same procedure for processing these files.

Reconciliation – Payroll Activity

Payroll accountants prepare a monthly reconciliation of payroll disbursements recorded in the core accounting system and payroll disbursements reported by the third-party payroll processors. The payroll accountant investigates and resolves any differences identified. This reconciliation is reviewed and approved by the supervisor or manager of Central Accounting Branch. In addition, ARC branch accountants prepare monthly GWA Account Statement reconciliations from the general ledger to Treasury's record. Any reconciliation differences identified by the branch accountant that prepares the GWA Account Statement reconciliation requiring correction are posted by another accountant or accounting technician in a subsequent accounting period. ARC supervisory accountants review and approve the GWA Account Statement/*Fund Balance with Treasury* reconciliations.

Customer Agency Control Considerations

Customer Agencies should establish controls to:

- Verify that payroll processed by third-party providers is complete and accurate.

- Review the financial reports provided by ARC to ensure that payroll disbursements are complete and accurate.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for the processing of payroll disbursements and observed ARC staff process disbursements, and determined that the processing was in accordance with the procedures.

- Inquired of the payroll accountant, observed the process of interfacing data from third-party payroll processors, and inspected the resultant interface error report. Determined that during the interface, input files were checked for errors and interface error reports were created if errors were identified. Additionally, determined that data would not interface until errors were corrected.

- For a selection of months, inspected payroll reconciliations and determined that reconciliations were performed and that any exceptions were resolved.

- For a selection of months, inspected GWA Account Statement reconciliations and determined that reconciliations were performed and that any exceptions were resolved.

No exceptions noted.

Control Objective 7 - USSGL

Controls provide reasonable assurance that transactions are processed in accordance with the U.S. Standard General Ledger (USSGL) and Treasury Financial Manual (TFM) guidance.

Description of Controls

ARC has documented procedures for processing transactions consistent with the USSGL.

Transaction Set-up Controls
ARC records proprietary and budgetary accounting entries using the USSGL at the transaction level. This is accomplished using a combination of transaction code, system setup, and data entry in ORACLE. In addition, ORACLE cross-validation rules have been established to prevent transactions from being processed to inappropriate USSGL accounts.

ARC follows the TFM to establish accounting transaction posting models in the core accounting system. System administrators require written authorization from a supervisor or manager to establish new posting models for transaction processing.

On an annual basis, ARC supervisors and managers review the USSGL Board's proposed and approved additions, deletions and/or modifications to USSGL account titles and/or account descriptions to determine their applicability to ARC Customer Agencies. Once the changes to the USSGL are approved by Treasury's FMS and the new TFM guidance is issued (generally mid-summer), ARC supervisors and managers communicate the appropriate changes to system administrators to ensure the accounting transaction posting models are properly revised. All USSGL related system modifications are completed by the start of the first accounting period of the new fiscal year.

General Ledger Account Reconciliations
Accountants perform general ledger account reconciliations (utilizing accounting system subledgers or Excel spreadsheets) on balances of certain material accounts such as Fund Balance with Treasury, Investments, and Equipment and Software, for supervisory review, to ensure related accounting transactions were posted to the appropriate general ledger accounts. ARC accountants prepare budgetary to proprietary account relationship reconciliations on a monthly basis, for supervisory review, to ensure complete general ledger account posting for all recorded transactions. An accounting technician or an accountant corrects invalid out-of-balance relationships.

FACTS I Edit Checks
ARC enters pre-closing adjusted trial balances for its non-Treasury customers, except for the Department of Homeland Security, into the FACTS I system at the Treasury appropriation/fund group level using USSGL accounts and attributes. Treasury's FMS maintains the FACTS I system. The FACTS I system checks that the trial balance has, in aggregate, equal debit and credit balances before the trial balance can be submitted in FACTS I. FACTS I also flags abnormal balances for scrutiny by an ARC accountant. After entering the adjusted trial balances into FACTS I, ARC reviews the submitted balances and resolves any invalid abnormal balances or out-of-balance conditions. Once any necessary corrections have been made, the accountant submits the adjusted trial balance into the FACTS I system.

FACTS II Edit Checks

ARC submits the FACTS II files for its non-Treasury customers, except for the Department of Homeland Security, using a bulk file upload. Accountants create the bulk files by running a job within the ORACLE application. ORACLE requires the data to pass several edit checks before it will create the bulk file. ARC manually uploads the FACTS II files into the FACTS II system. Treasury's FMS maintains the FACTS II system. The FACTS II system performs USSGL edit checks and rejects any files that fail the edit checks. ARC investigates and resolves any files rejected by the FACTS II system.

Treasury Information Executive Repository (TIER) Validation Checks

For ARC's Treasury and the Department of Homeland Security Customer Agencies, FACTS I and II reporting requirements are met using TIER. TIER is Treasury's departmental data warehouse that receives monthly uploaded financial accounting and budgetary data from the Treasury bureaus and other reporting entities within the Department of the Treasury in a standardized format. Data submitted to TIER by an ARC accountant is validated based on system-defined validation checks.

ARC has customized programs in its core accounting system that extract the accounting and budgetary data in the required TIER format. TIER has a standardized chart of accounts that is compliant with USSGL guidance issued by the Department of the Treasury. FACTS II edit checks are incorporated in the TIER validation checks. After submitting the adjusted trial balances into TIER, ARC accountants review the edit reports and resolve any invalid attributes or out-of-balance conditions. ARC accountants document this review by completing the TIER Submission Checklist, which is further reviewed by a supervisor.

Financial Statement Crosswalks

ARC accountants prepare a *Balance Sheet, Statement of Net Cost* and *Statement of Budgetary Resources* for all Customer Agencies that are entities of Chief Financial Officer Act agencies and the Accountability of Tax Dollars Act of 2002. The statements are to be submitted each quarter to the Director of the Office of Management and Budget (OMB) and the Congress. Additionally, ARC accountants prepare the *Statement of Changes in Net Position, Statement of Financing* and *Statement of Custodial Activity* (when applicable) for all Customer Agencies. ARC accountants compare FMS financial statement crosswalks to ARC's internally prepared financial statements to ensure compliance with the reporting requirements. ARC investigates and resolves any differences between Treasury's financial statement crosswalk and ARC's internally prepared financial statements.

FARS Statement Review

For Treasury Customer Agencies, quarterly financial statements are generated using the data submitted in the quarter end TIER submission. Treasury's Financial Analysis and Reporting System (FARS) produces the statements (except for the *Statement of Financing*) using data bureaus have submitted to TIER and Treasury submits consolidated statements to OMB. ARC accountants compare the financial statements prepared by FARS to internally prepared financial statements and resolve any differences. Accountants also prepare and submit the *Statement of Financing* in a Treasury-provided Excel template to staff at the departmental level for consolidation. The *Statement of Financing* is reviewed by an ARC supervisory accountant prior to submission to Treasury, as is the accountant's comparison of FARS statements to the internally prepared financial statements.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for the processing of transactions consistent with the USSGL and determined that procedures were documented.

- Inspected a list of users with access to change posting models and inquired of ARC management and determined that access was limited commensurate with job responsibilities.

- For a selection of posting model changes and additions, inspected ARC supervisory approval of the changes and inspected TFM/USSGL guidance. Determined that the changes and additions were authorized and that they were in agreement with TFM/USSGL guidance.

- For a selection of months, inspected monthly general ledger account reconciliations and determined that reconciliations were performed and that any exceptions were resolved.

- For a selection of months, inspected a budgetary to proprietary account relationship reconciliations and determined that reconciliations were performed and that any exceptions were resolved.

- Inquired of ARC staff and observed the staff review FACTS I edit check reports, and determined that ARC staff reviewed FACTS I edit reports and resolved any invalid attributes or out-of-balance conditions.

- Inquired of an ARC accountant and observed them run the ORACLE job that creates the FACTS II bulk data upload file, and determined that ORACLE edit checks were applied to the data, and that the ARC accountant resolved any exceptions.

- Inquired of ARC staff and observed the staff review FACTS II edit check reports, and determined that ARC staff reviewed FACTS II edit reports and resolved any invalid attributes or out-of-balance conditions.

- For a selection of months, inspected TIER Submission Checklists for evidence of ARC supervisory review of TIER data and timeliness of submission and determined that submissions had been reviewed.

- For a selection of months, inspected reconciliations of ARC-prepared financial statements to the Treasury financial statement crosswalks and determined that reconciliations were performed and that any exceptions were resolved.

- For a selection of months, inspected reconciliation of financial statements prepared by FARS to internally prepared financial statements and determined that reconciliations were performed and that any exceptions were resolved.

- For a selection of months, inspected *Statement of Financing* reports and determined that they were reviewed by a supervisory accountant before submission.

No exceptions noted.

Control Objective 8 - Accruals

Controls provide reasonable assurance that the period-end accruals are authorized, processed timely, reviewed, reconciled, and properly documented in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures for staff to follow for the processing of accruals.

Customer Review of Revenue and Expense Accruals
Accounting technicians record period-end accruals for goods and services provided/received, but not billed/invoiced, in the core accounting system based on instruction provided from the Customer Agency.

For all Customer Agencies, except the Treasury Franchise Fund, accounting technicians record period-end accruals for goods and services provided, but not billed in the accounting system through standard accrual transactions. For Treasury Franchise Fund Customer Agencies, accounting technicians record period-end accruals for goods and services provided but not billed in ORACLE using an automated journal entry process. The amounts recorded are based on information provided by e-mail from the Customer Agency. Accounting technicians enter information received from the Customer Agency into a spreadsheet template. An accountant reviews the spreadsheet and converts it into a data file that is automatically loaded into ORACLE and reviewed and approved by a supervisory accountant.

Non-Invoice Accrual Reviews
Accountants record non-invoice related expense accruals for employee benefits, such as workers' compensation and leave liability in ORACLE. The workers' compensation accruals are based on historical trend analysis and/or actual costs incurred. The leave liability accruals are based on data provided by the Customer Agency's payroll provider or Human Resources office. For applicable Customer Agencies, the ARC payroll accountant processes payroll leave accrual entries using a batch interface that posts summary payroll data to the core accounting system. For non-batch interfaced leave accruals, a supervisory accountant reviews the accrued employee benefits to determine that the accrual is processed and posted.

Scorecard Review
Treasury's monthly data scorecard verifies that certain non-invoice related expense accruals are recorded on at least a quarterly basis. Supervisory accountants validate the quality of TIER data by reviewing an ARC accountant-prepared TIER Submission Checklist, which includes verification that non-invoice related expense accruals are posted at least quarterly. Additionally, both ARC supervisory accountants and managers monitor the quality of the data submitted by reviewing Treasury’s monthly data quality scorecard. If non-invoice related expense accruals are not recorded at least quarterly, the reviewer contacts the ARC Customer Agency reporting accountant to research the non-invoice related expense accrual posting.

General Ledger to Subledger Reconciliation
On a monthly basis, ARC accountants prepare a reconciliation of revenue and expense accrual balances in the general ledger to the subledger detail, which is reviewed by a supervisor. Accountants reconcile only billed revenue accruals since unbilled revenue accruals are recorded

directly in the general ledger. Any differences identified are corrected by an accounting technician or accountant in the subsequent accounting period.

Budget Execution System Controls

Customer Agencies can establish and monitor both legally established and internally developed budget plans in ORACLE to ensure obligations are properly authorized and recorded. Budget plans can be established at the following levels of the accounting structure in ORACLE:

- Appropriation/Fund (Based upon the customer's appropriation)
- Apportionment (Based upon the apportionment schedule on the SF132)
- Cost Center (Based upon the customer's internal budget plan)
- Reporting Category (Based upon the customer's internal budget plan)
- Project Code (Based upon the customer's internal budget plan)
- Budget Object Code (Based upon the customer's internal budget plan)

Budget execution system controls can be set to prevent spending beyond the budget plan amount or allow spending over the budget plan amount at any level of the budget plan. Spending beyond the apportionment and appropriation levels (legal levels) are prohibited. Decisions on control settings that permit or prevent spending beyond other budget plan levels are made by the Customer Agency. System controls are applied at the fund level after passage of appropriation legislation until a customer agency provides an appropriate financial plan. Upon receipt and input of the budget plan, controls will be established at the detail level dictated by the Customer Agency.

Budget execution settings are determined by the Customer agency and input into ORACLE by the CSB. System settings are reviewed with the Customer Agency on an annual basis. Budget plans are input into ORACLE by ARC staff, based upon budget plans provided by Customer Agencies.

Document Numbering

All accounting entries recorded in ARC's core accounting system require a transaction or document identification number. System controls prohibit the use of duplicate document numbers on revenue and expense accruals. ARC has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of ARC reports to better identify and/or determine the nature of transactions processed by ARC. When an ARC user attempts to enter a transaction identification number that already exists, the accounting system issues an error message that alerts the user of the duplication.

Customer Agency Control Considerations

Customer Agencies should establish controls to:

- Review open accrual reports for completeness, accuracy, and validity.

- Approve and send revenue and expense accruals to ARC in a timely manner.

- Communicate Customer Agency required levels of budget and spending controls to ARC.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for the processing of accruals and observed ARC staff processing accruals, and determined that the processing was in accordance with the procedures.

- For a selection of accruals, inspected documentation of Customer Agency authorization and determined that the accruals were authorized and processed timely.

- For a selection of months for Treasury Franchise Fund Customer Agencies, inspected Treasury Franchise Fund Customer spreadsheets and determined that the submissions were reviewed and approved by a supervisory accountant.

- For a selection months, inspected leave liability accruals documentation and determined that the accrual was prepared based on data provided by the Customer Agencies and was reviewed by a supervisor.

- Inquired of a supervisory accountant and inspected Treasury-issued scorecards for the examination period, and determined that the entities reported accruals at least quarterly.

- For a selection of months, inspected reconciliation of revenue and expense accrual balances in the general ledger to the sub ledger detail and determined that reconciliations were performed and that any exceptions were resolved.

- For a selection of budget execution settings that were input during the review period, inspected evidence of Customer Agency review and the instructions from the Customer Agency, and compared them to the Discoverer reports detailing the budget settings. Determined that the budget execution settings input by ARC were reviewed and authorized by the Customer Agency.

- Observed ARC staff attempt to enter a budget transaction into ORACLE in excess of a budget limit and noted that the system prevented the entry.

- Observed an ARC staff member attempt to enter a transaction into ORACLE with a document number that had already been entered into ORACLE and noted that ORACLE automatically rejected the entry of a duplicate document number.

No exceptions noted.

Control Objective 9 – Government-Wide Reporting

Controls provide reasonable assurance that Government-wide reporting is performed in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures for staff to follow for the preparation of government-wide reports.

FACTS I & II

ARC policies require the submission of *FACTS I* and *FACTS II* reports based on FMS's criteria for these applications. All reports must pass all FACTS edit checks. For non-Treasury Customer Agencies, except the Department of Homeland Security, supervisory accountants review all submissions prepared by accountants and review all data to ensure all reporting deadlines are met. All fourth quarter FACTS II submissions require certification by an ARC supervisor or manager, or other designated Customer Agency representative.

TIER

Treasury reporting entities are required to submit financial accounting and budgetary data each month to the Treasury's data warehouse, TIER, by the third business day of the subsequent month. The Department of Homeland Security reporting entities are required to submit financial accounting and budgetary data each month to Treasury's data warehouse, TIER, by the fifth business day of the subsequent month. To meet this requirement, ARC performs the ORACLE month-end close processes on the second business day after the end of the month. Supervisory accountants validate the quality of TIER data to ensure reporting deadlines are met by reviewing an accountant-prepared TIER Submission Checklist. The TIER Submission Checklist consists of internally and Treasury-defined data quality standards. Additionally, both supervisory accountants and managers monitor the quality of the data submitted by reviewing Treasury's monthly data quality scorecard.

EFT and Prompt Payment

ARC follows the Treasury guidelines for the *EFT* and *Prompt Payment* reports for its Treasury customers. ARC accountants prepare these reports on a monthly basis. Supervisory accountants review these reports before submission. Treasury also requires that a Customer Agency representative sign the *Prompt Payment* reports.

Financial Statements

ARC accountants prepare a *Balance Sheet, Statement of Net Cost* and *Statement of Budgetary Resources* for all Customer Agencies that are entities of Chief Financial Officer Act agencies and the Accountability of Tax Dollars Act of 2002. The statements are to be submitted each quarter to the Director of the OMB and the Congress. Additionally, ARC accountants prepare the *Statement of Changes in Net Position, Statement of Financing* and *Statement of Custodial Activity* (when applicable) for all Customer Agencies. ARC accountants compare FMS financial statement crosswalks to ARC's internally prepared financial statements to ensure compliance with the reporting requirements. ARC investigates and resolves any differences between Treasury's financial statement crosswalk and ARC's internally prepared financial statements.

FARS

For Treasury Customer Agencies, quarterly financial statements are generated using the data submitted in the quarter-end TIER submission. Treasury's FARS produces the statements (except for the *Statement of Financing*) using data Bureaus have submitted to TIER and Treasury submits consolidated statements to OMB. ARC accountants compare the financial statements prepared by FARS to internally prepared financial statements and resolve any differences. Accountants also prepare and submit the *Statement of Financing* in a Treasury-provided Excel template to staff at the departmental level for consolidation. The *Statement of Financing* is reviewed by an ARC supervisory accountant prior to submission to Treasury, as is the accountant's comparison of FARS statements to the internally prepared financial statements.

Receivables

ARC Accountants prepare and submit a quarterly *Report on Receivables Due from the Public* for all Customer Agencies. The report is reviewed by an ARC supervisory accountant prior to submission to Treasury.

Customer Agency Control Considerations

Customer Agencies should establish controls to:

- Review the financial reports prepared by ARC to ensure that all reports prepared for external use are complete, accurate, and submitted in a timely manner.

- Provide certification of *FACTS II* to ARC prior to ARC's *FACTS II* system certification

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for the preparation of government-wide reporting and determined that procedures were documented.

- For a selection of submissions, inspected evidence of supervisory accountant review of FACTS I and FACTS II submissions and determined that submissions were reviewed.

- For a selection of fourth quarter FACTS II submissions, inspected evidence of management review and determined that they were reviewed and certified.

- For a selection of months, inspected TIER Submission Checklists for evidence of ARC supervisory review of TIER data and timeliness of submission and determined that submissions had been reviewed.

- For a selection of months, inspected *EFT* and *Prompt Payment* reports and determined that they were reviewed by a supervisory accountant before submission.

- For a selection of months, inspected reconciliations of ARC-prepared financial statements to the Treasury financial statement crosswalks and determined that reconciliations were performed and that any exceptions were resolved.

- For a selection of months, inspected reconciliations of financial statements prepared by FARS to internally prepared financial statements and determined that reconciliations were performed and that any exceptions were resolved.

- For a selection of months, inspected *Statement of Financing* reports and determined that they were reviewed by a supervisory accountant before submission.

- For a selection of quarters, inspected *Report on Receivables Due from the Public* reconciliations and determined that reconciliations were documented and that any exceptions were resolved.

- For a selection of quarters, inspected *Reports on Receivables Due from the Public* and determined that they were reviewed by an ARC supervisory accountant.

No exceptions noted.

Control Objective 10 – Administrative Spending

Controls provide reasonable assurance that administrative spending controls are reviewed, reconciled, and documented in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures related to administrative spending controls.

Budget Execution System Controls

Customer Agencies can establish and monitor both legally established and internally developed budget plans in ORACLE to ensure obligations are properly authorized and recorded. Budget plans can be established at the following levels of the accounting structure in ORACLE:

- Appropriation/Fund (Based upon the customer's appropriation)
- Apportionment (Based upon the apportionment schedule on the SF132)
- Cost Center (Based upon the customer's internal budget plan)
- Reporting Category (Based upon the customer's internal budget plan)
- Project Code (Based upon the customer's internal budget plan)
- Budget Object Code (Based upon the customer's internal budget plan)

Budget execution system controls can be set to prevent spending beyond the budget plan amount or allow spending over the budget plan amount at any level of the budget plan. Spending beyond the apportionment and appropriation levels (legal levels) are prohibited. Decisions on control settings that permit or prevent spending beyond other budget plan levels are made by the Customer Agency. System controls are applied at the fund level after passage of appropriation legislation until a customer agency provides an appropriate financial plan. Upon receipt and input of the budget plan, controls will be established at the detail level dictated by the Customer Agency.

Budget execution settings are determined by the Customer agency and input into ORACLE by the CSB. System settings are reviewed with the Customer Agency on an annual basis. Budget plans are input into ORACLE by ARC staff, based upon budget plans provided by Customer Agencies.

Reconciliation – Budgetary and Proprietary Account Relationships

ARC accountants prepare budgetary to proprietary account relationship reconciliations on a monthly basis, for supervisory review, to ensure complete general ledger account posting for all recorded transactions. An accounting technician or an accountant corrects invalid out-of-balance relationships.

Reconciliation – Fund Balance With Treasury

A Federal Agency's FBWT assists the agency in monitoring use of budget authority. Treasury's FMS provides the following reports to inform agencies of their FBWT and to assist agencies in reconciling their general ledger balances to FMS balances:

- *Statement of Differences (Disbursements/Deposits)* provides the net difference between FMS's control totals and the agency's SF 224 submission.
- GWA Account Statement (Transactions) provides increases and decreases to balances, detailed at the submitting ALC levels.
- GWA Account Statement (Account Summary) provides beginning balance, current month net activity and ending balance.

ARC accountants reduce the probability of month-end differences relating to disbursements by comparing preliminary SF 224 disbursement data to month-to-date data obtained from CA$HLINK II, RFC Agency Link and IPAC systems. Any differences identified by the accountant are corrected by an accounting technician or another accountant prior to the close of the accounting period.

ARC accountants perform *Statement of Differences* reconciliations, for supervisory review, as well as GWA Account Statement balances to general ledger cash balances. Supervisors verify total receipts and disbursements on the SF 224 agree with the FMS and IPAC schedules. Supervisors also verify the total general ledger cash balance in ORACLE agrees with the reconciliation and the GWA Account Statement balance agrees with the reconciliation. If differences are identified during the reconciliations, ARC accountants determine the cause of the difference and the action, if any, that is needed to resolve the discrepancy. If the difference requires correction, an entry is posted in the accounting system by an accounting technician or another accountant.

Customer Agency Control Considerations

Customer Agencies should establish controls to:

- Properly approve and accurately enter obligations into the procurement and travel systems in the proper period.

- Send valid requests to record manual obligations to ARC in a timely manner.

- Review open obligation reports for completeness, accuracy, and validity.

- Restrict Customer Agency access to ORACLE, Discoverer, PRISM, webTA, and GovTrip to authorized individuals.

- Communicate Customer Agency required levels of budget and spending controls to ARC.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures related to administrative spending, inspected reconciliations, and observed ARC staff process transactions, and determined that processing was in accordance with the procedures.

- For a selection of budget execution settings that were input during the review period, inspected evidence of Customer Agency review and the instructions from the Customer Agency, and compared them to the Discoverer reports detailing the budget settings. Determined that the budget execution settings input by ARC were reviewed and authorized by the Customer Agency.

- Observed ARC staff attempt to enter a budget transaction into ORACLE in excess of a budget limit and noted that the system prevented the entry.

- For a selection of months, inspected a budgetary to proprietary account relationship reconciliations and determined that reconciliations were performed and that any exceptions were resolved.

- For a selection of months, inspected SF 224 reconciliations and determined that reconciliations were documented and that any exceptions were resolved.

- For a selection of months, inspected FMS 6652, *Statement of Difference* reconciliations and determined that reconciliations were documented and that any exceptions were resolved.

- For a selection of months, inspected payroll reconciliations and determined that reconciliations were performed and that any exceptions were resolved.

- For a selection of months, inspected GWA Account Statement reconciliations and determined that reconciliations were performed and that any exceptions were resolved.

- For a selection of months, inspected monthly general ledger account reconciliations and determined that reconciliations were performed and that any exceptions were resolved.

No exceptions noted.

Control Objective 11 – Budget

Controls provide reasonable assurance that budget entries are properly documented and processed in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures for staff to follow for the processing of budget entries.

Budget Documentation
For Customer Agency appropriations subject to annual enactment, ARC enters an appropriation based on the amount approved in the annual appropriations process, as supported by the automatic amount calculated during a continuing resolution (CR), the enacted appropriation legislation, or Treasury documentation. ARC enters an apportionment in ORACLE from the Customer Agency's SF 132, Apportionment and Reapportionment Schedule. Upon receipt of the Customer Agency's budget plan or reprogramming guidance, ARC allocates funding to the Customer Agency's accounting values according to the detail provided by the customer.

For Customer Agency sources of funds that are not subject to the annual appropriations process, such as reimbursable or revolving accounts, ARC enters an appropriation and apportionment based on the Customer Agency's SF 132 and recorded reimbursable activity for those accounts subject to the apportionment process. ARC allocates funding to the Customer Agency's accounting values based on the Customer Agency's budget plan or recorded reimbursable activity. For sources of funds not subject to both the annual appropriations process and the apportionment process, ARC enters an appropriation and apportionment at the fund level and allocates funding to the Customer Agency's accounting values based on the Customer Agency's budget plan, recorded reimbursable activity, or reprogramming guidance.

Budget Execution System Controls
Customer Agencies can establish and monitor both legally established and internally developed budget plans in ORACLE to ensure obligations are properly authorized and recorded. Budget plans can be established at the following levels of the accounting structure in ORACLE:

- Appropriation/Fund (Based upon the customer’s appropriation)
- Apportionment (Based upon the apportionment schedule on the SF132)
- Cost Center (Based upon the customer’s internal budget plan)
- Reporting Category (Based upon the customer’s internal budget plan)
- Project Code (Based upon the customer’s internal budget plan)
- Budget Object Code (Based upon the customer’s internal budget plan)

Budget execution system controls can be set to prevent spending beyond the budget plan amount or allow spending over the budget plan amount at any level of the budget plan. Spending beyond the apportionment and appropriation levels (legal levels) are prohibited. Decisions on control settings that permit or prevent spending beyond other budget plan levels are made by the Customer Agency. System controls are applied at the fund level after passage of appropriation legislation until a customer agency provides an appropriate financial plan. Upon receipt and input of the budget plan, controls will be established at the detail level dictated by the Customer Agency.

Budget execution settings are determined by the Customer agency and input into ORACLE by the Business Technology Division’s Customer Service Branch (CSB). System settings are reviewed with the Customer Agency on an annual basis. Budget plans are input into ORACLE by ARC staff, based upon budget plans provided by Customer Agencies.

Reconciliation – Budgetary and Proprietary Account Relationships

ARC accountants prepare budgetary to proprietary account relationship reconciliations on a monthly basis, for supervisory review, to ensure complete general ledger account posting for all recorded transactions. An accounting technician or an accountant corrects invalid out-of-balance relationships.

Reconciliation – Fund Balance With Treasury

A Federal Agency's FBWT assists the agency in monitoring budget authority. Treasury's FMS provides the following reports to inform agencies of their FBWT and to assist agencies in reconciling their general ledger balances to FMS balances:

- GWA Account Statement (Transactions) provides increases and decreases to balances, detailed at the submitting ALC levels.
- GWA Account Statement (Account Summary) provides beginning balance, current month net activity and ending balance.

ARC accountants perform reconciliations, for supervisory review, of GWA Account Statement balances to general ledger cash balances. Supervisors verify the total general ledger cash balance in ORACLE agrees with the reconciliation and the GWA Account Statement balance agrees with the reconciliation. If differences are identified during the reconciliations, ARC accountants determine the cause of the difference and the action, if any, that is needed to resolve the discrepancy. If the difference requires correction, an entry is posted in the accounting system by an accounting technician, another accountant or a budget analyst.

Document Numbering

All accounting entries recorded in ARC's core accounting system require a transaction or document identification number. ARC has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of ARC reports to better identify and/or determine the nature of transactions processed by ARC.

Customer Agency Control Considerations

Customer Agencies should establish controls to:

- Review the financial reports provided by ARC to ensure that budget entries are complete and accurate.

- Send approved budget plans to ARC in a timely manner.

- Communicate Customer Agency required levels of budget and spending controls to ARC.

- Communicate OMB apportionment status to ARC.

- Monitor usage of budget authority during periods of operation under a Continuing Resolution to ensure that OMB directed apportionment limits are not exceeded.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for processing budget entries and determined that procedures were documented.

- For a selection of customer budget entries, inspected the supporting documentation and determined that the budget entries were processed in accordance with the supporting documentation.

- For a selection of budget execution settings that were input during the review period, inspected evidence of Customer Agency review and the instructions from the Customer Agency, and compared them to the Discoverer reports detailing the budget settings. Determined that the budget execution settings input by ARC were reviewed and authorized by the Customer Agency.

- Observed ARC staff attempt to enter a budget transaction into ORACLE in excess of a budget limit and noted that the system prevented the entry.

- Observed an ARC staff member attempt to enter a transaction into ORACLE with a document number that had already been entered into ORACLE and noted that ORACLE automatically rejected the entry of a duplicate document number.

No exceptions noted.

Control Objective 12 – Manual Journal Entries

Controls provide reasonable assurance that manual journal entries are properly authorized.

Description of Controls

ARC has documented procedures for staff to follow for the processing of manual journal entries.

Journal Entry Approval
A user's profile in ORACLE determines whether or not the user can prepare and/or approve a manual journal entry. ORACLE system controls require that all manual journal entries be routed to an approver. Once a user has entered a journal entry, ORACLE automatically routes the journal entry to their supervisor's approval queue.

Document Numbering
ORACLE assigns all manual journal entries a specific journal category and journal source and ARC follows a standard document numbering scheme. Hardcopy documentation supporting the journal entry accompanies each request for approval and is maintained with a journal entry log. The approver compares the hardcopy documentation to ORACLE and approves the journal entry.

Customer Agency Control Considerations

- Send valid requests to record manual journal entries to ARC in a timely manner.
- Maintain and communicate to ARC, a list of individuals authorized to submit manual journal entries that are initiated by the Customer Agency.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for processing manual journal entries and observed the processing of manual journal entries, and determined that processing was in accordance with the procedures.
- For a selection of users with access to approve manual journal entries in ORACLE, inquired of ARC management and determined that the access privileges were commensurate with job responsibilities.
- Observed an ORACLE user with authority to approve manual journal entries prepare a manual journal entry and noted that ORACLE automatically routed the journal entry to the approval queue of the user's supervisor and did not present an opportunity for the user to approve their own manual journal entry.
- Inspected the configuration of user accounts and determined that ORACLE was configured to deny users the ability to approve their own manual journal entries.
- For a selection of manual journal entries, inspected hardcopy supporting documentation and related ORACLE journal entries and determined that the manual journal entries were properly authorized.

No exceptions noted.

GENERAL COMPUTER CONTROLS

Control Objective 13 – System Access

Controls provide reasonable assurance that systems are protected from unauthorized access in accordance with ARC policies and procedures.

Description of Controls

ARC follows BPD policies and procedures that were developed, documented, disseminated, and that are periodically reviewed and updated to facilitate the implementation of logical access controls. Additionally, procedures specific to ORACLE, PRISM, webTA and GovTrip have been documented. The logical access controls are based on Treasury and BPD policies and standards (Treasury Information Technology Security Program TDP-85-01 Volumes I and II), which, in turn, are based on the applicable Federal laws and regulations. These controls are the system-based mechanisms that are used to specify which individuals and/or processes are to have access to a specific system resource and the type of access that is to be permitted. These controls limit user access to information and restrict their system access to their designated level.

ORACLE

Access to ORACLE is restricted to users with a valid logon ID and password. ORACLE logons/sessions are encrypted to protect the information, making it unintelligible to all but the intended users. Sessions are protected using 128-bit Secure Sockets Layer (SSL) encryption. Prospective ORACLE users must complete, sign and submit a supervisor-approved *Administrative Resource Center System Access Form for End User Applications* to request access to ORACLE. The end user's signature indicates that they are familiar with the Privacy Act information and security requirements and will comply with computer security requirements established by BPD and ARC. The form defines the user's access specifications, which will allow the user to perform his/her duties in ORACLE. Changes to existing user profiles require an e-mail to be sent to the ORACLE Support Team Security mailbox by the user's supervisor/manager requesting the change, and defining what access should be added/deleted/changed. In order to remove a user's access, customer agencies submit a request for account termination. At that time, the ORACLE user account is end-dated in the system to remove their access. Additionally, each day the ORACLE Support Team generates and reviews a list of ORACLE user accounts that have been inactive for 110 days. An e-mail is sent to the user warning them that their account will be end-dated if they maintain an inactive status for 120 days. After 120 days of inactivity the user's account will be end-dated. Annually, the ORACLE Support Team sends out a list of users to each customer agency to initiate a periodic review of access. The ORACLE Support Team updates the permissions for users based on the responses received from the customer agencies.

Access within ORACLE is further limited to specific operating units within ORACLE that contain detailed accounting records of specific ARC customers. These restrictions limit the ability to add or modify existing records of specific ARC customers, allowing only users assigned to maintain these records the ability to view and/or change data.

Only CSB and QCB employees are assigned the System Administrator responsibility in the ORACLE application. The employees with the System Administrator responsibility have limited access to perform operational functions in ORACLE, specifically limited to the month-end closing, during customer conversions (as directed by the functional teams) or emergency situations that can be approved by a supervisor or manager after the fact. ARC management approved both functional and system administrator rights for certain ARC employees and consultants who participated in the United States Mint conversion. Additionally, the individuals with ORACLE System Administrator privileges perform multiple functions, including that of the ORACLE Support team members. As a result, these individuals periodically require temporary access privileges of a functional user in order to address user inquiries. An edit check prevents an ORACLE System Administrator from adding or removing any responsibilities from their own user ID.

Updates to a user's ORACLE responsibilities are audited by the PRISM Support team on a daily basis. The PRISM Support team reviews the changes to functional access privileges and compares the changes to BTD's Team Responsibilities matrix to determine whether or not the access privileges are appropriate. Follow up is performed to validate the addition of any privileges that are not on the BTD's Team Responsibilities matrix.

The CSB/QCB managers can be assigned the System Administrator responsibility in situations where the manager deems the access is required. This responsibility is granted on a temporary basis with the proper request and approval and will be end-dated once the access is no longer necessary. PTSB can be assigned System Administrator responsibility when the developers deem the access is required. This responsibility is granted on a temporary basis with the proper request and approval and will be end-dated once the access is no longer needed.

Administrative access to the underlying ORACLE servers and databases is limited to server and database administrators within the OIT and specific BTD employees.

ORACLE uses a multi-org functionality to strengthen security within the application. Each Customer Agency is setup as an operating unit in ORACLE. When a new responsibility is created by the system administrators, it is mapped to a specific operating unit by a system profile option. The multi-org functionality helps ensure that a user assigned to a responsibility (which in turn is mapped to an operating unit) can only see or enter data for that customer (or operating unit). ORACLE also provides a value set security feature, assigned to a responsibility, which further controls new data entry in the operating unit by limiting the list of values (LOV) for the accounting flexfield to those values specific to the customer (or operating unit).

User Identifications (IDs) are assigned to BPD employees consistent with their network logon ID. User IDs for Customer Agency staff are assigned by an ARC system administrator. A temporary password is assigned to BPD users by an e-mail sent through BPD's intranet. A temporary password is assigned to new ARC Customer Agency staff by calling the ORACLE Support Desk. ORACLE Support Desk personnel are responsible for verifying the caller's identity. Access can only be restored by following the original steps of obtaining a temporary password. Once the user logs onto the accounting system, they must establish their own unique password, which must be a combination of eight alpha/numeric characters, no repeating characters, and may not include the user name. Passwords may not be reused for 600 days. Accounting system controls require the assignment of a new password as follows: System Administrators – every 30 days; all other users – every 90 days. Failure to provide the appropriate password after three attempts will lock the user out of the system. The user must contact the ORACLE Support Desk to have their password reset. If the user's current session is inactive for 15 consecutive minutes (setting is 30 consecutive minutes for the US Mint's instance of ORACLE), they will be timed out of the system and will have to log back into the system.

ORACLE access attempt logs are reviewed daily by the PRISM Support team to identify if users attempted to unsuccessfully access the system five or more times in the day. If additional follow up is required, an e-mail is sent to the user indicating that the access attempts were noted and requesting that the user notify ARC if the attempts were not made by the user.

PRISM

Access to PRISM is restricted to users with a valid logon ID and password. PRISM logons/sessions are encrypted to protect the information, making it unintelligible to all but the intended users. Sessions are protected using 128-bit SSL encryption. Prospective PRISM users must complete, sign, and submit a supervisor-approved *Administrative Resource Center System Access Form for End User Applications* to request access to PRISM. The end user's signature indicates that they are familiar with the Privacy Act information and security requirements and will comply with computer security requirements established by BPD and ARC. The form defines the user's access specifications, which will allow the user to perform his/her duties in PRISM. Changes to existing user profiles require an e-mail to be sent to the PRISM Support Team mailbox by an authorized individual at the customer agency, requesting the change, and defining what access should be added/deleted/changed. In order to remove a user's access, customer agencies submit a request for account termination. At that time, the PRISM user is end-dated in the system to remove their access. Additionally, each day the ORACLE Support Team generates and reviews a list of PRISM user accounts that have been inactive for 110 days. An e-mail is sent to the user warning them that their account will be end-dated if they maintain an inactive status for 120 days. After 120 days of inactivity the user's account will be end-dated. Annually, the PRISM Support Team sends out a list of users to each customer agency to initiate a periodic review of access. The PRISM Support Team updates the access according to the responses received from the customer agencies.

User access within PRISM is further limited by only allowing users to approve the addition or modification of records to the operating units they have been assigned in ORACLE. The System Administrator responsibility in PRISM is limited to certain employees requiring the access for the performance of job duties. Administrative access to the underlying PRISM servers and databases is limited to server and database administrators within the OIT and specific BTD employees. PRISM utilizes the existing security features and functionality of ORACLE. For example, new users are setup in ORACLE and assigned appropriate PRISM responsibilities. Within ORACLE, the responsibilities are mapped to PRISM security groups. The user and security groups then flow to PRISM. Within the PRISM application, users are assigned additional responsibilities as authorized on the access form.

User IDs are assigned to BPD employees consistent with their network logon ID. User IDs for Customer Agency staff who utilize PRISM are assigned by an ARC system administrator. A temporary password is assigned to BPD users by an e-mail sent through BPD's intranet. A temporary password is assigned to new ARC Customer Agency staff by calling the PRISM Support Desk. PRISM Support Desk personnel are responsible for verifying the caller's identity prior to establishing the user's password. Once the user logs onto the system, they must establish their own unique password, which must be a combination of eight or more alpha/numeric characters, and may not match the user name. Passwords may not be reused for 720 days. Accounting system controls require the assignment of a new password as follows: System Administrators – every 30 days; all other users – every 90 days. Failure to provide the appropriate password after three attempts will lock the user out of the system. The user must contact the PRISM Support Desk to have their password reset. If the user's current session is inactive for 20 consecutive minutes, they will be timed out of the system and will have to log back into the system.

PRISM access attempt logs are reviewed daily by the ORACLE Support team to identify if users attempted to unsuccessfully access the system five or more times in the day. If additional follow up is required, an e-mail is sent to the user indicating that the access attempts were noted and requesting that the user notify ARC if the attempts were not made by the user.

webTA[1]

Access to webTA is restricted to users with a valid logon ID and password. Access to webTA is provided using 128-bit SSL encryption. All personnel require access to webTA in order to complete time and attendance submission. Users granted standard employee access privileges do not require the submission of an access form. However, users that require elevated access privileges (e.g., timekeeper, supervisor) are added to the webTA system following receipt of a supervisor-approved *Administrative Resource Center System Access Form for End User Applications*. The end user's signature indicates they are familiar with the Privacy Act information and security requirements and will comply with computer security rules. The form defines the user's access specifications, which will allow the user to perform his/her duties in webTA. Changes to existing user profiles require a new access form to be submitted by the Customer Agency. Upon receipt of an *Administrative Resource Center System Access Form for End User Applications* requesting the deletion of a webTA user or upon receipt of a timesheet coded as "Final", an HR Administrator in PLSB removes the assigned responsibilities. Annually, an HR Administrator sends out a list of timekeepers and supervisors to each customer agency for use by the customer agency to perform a periodic review of access. The list is limited to those timekeepers and supervisors that are not responsible for validating or approving time for a member of the customer agency.

User access within webTA is further limited by the role they are assigned in the system (i.e., Employee, Timekeeper, Supervisor, etc.). The System Administrator and HR Administrator roles in webTA are limited to certain employees, ensuring no one serves in both administrator roles. Periodically, there is a need for the System Administrator to research a problem in a production instance using an HR Role. When such an event arises the System Administrator can be temporarily granted HR specific roles with supervisor approval. Administrative access to the underlying webTA servers and databases is limited to server and database administrators within the OIT.

An HR Administrator assigns user IDs to BPD employees consistent with their network logon ID. User IDs for Customer Agency staff who utilize webTA as timekeepers or supervisors are also assigned by an HR Administrator. An HR Administrator also assigns a temporary password to users by an e-mail. The temporary password provided in the e-mail includes "XXXX" and the user is instructed to replace the "XXXX" with the last four digits of their Social Security Number. Once the user logs onto the system, they must establish their own unique password, which must be a combination of eight or more alpha/numeric characters; must include at least one uppercase, one lowercase, one number, and one special character; and may not match the user name. Users are required to change their passwords every 90 days. Passwords may not be reused for 365 days. Failure to provide the appropriate password after three attempts will lock the user out of the system. The user must contact the Human Resources Support Desk to have their password reset. If the user's current session is inactive for 15 consecutive minutes, they will be timed out of the system and will have to log back into the system.

[1] The scope of the description of webTA controls applies only to full service webTA customers.

GovTrip

Access to GovTrip is restricted to users with a valid login ID and password. All users must complete the self-registration process and upon registering in GovTrip, if the criteria information entered when self-registering matches the criteria information in an existing profile that is confirmed in the database, the one-time use account token will be automatically e-mailed to the user. If the criteria information entered does not match, the account token will be forwarded to the user by the TSD helpdesk after verification. The criteria information includes first name, last name, e-mail address, and organization. After registration is completed, a Travel Services Division (TSD) Administrator verifies the request of the user to grant access to GovTrip. Budget Reviewers and Approving Officials must complete, sign, and submit a supervisor-approved *Administrative Resource Center Online Applications Access Request* or have a supervisor or agency travel contact authorize access via e-mail. The end user's signature indicates they are familiar with the Privacy Act information, security requirements, and will comply with computer security requirements established by BPD and ARC. The form defines the user's access specifications, which will allow the user to perform his/her duties in GovTrip. Changes to a user's identification (i.e., name change) or to the user's role in GovTrip require an *Administrative Resource Center Online Applications Access Request* to be resubmitted or an e-mail from the user copying his/her approving official. Upon receipt of an Exit Clearance form or e-mail request, GovTrip access permissions are set to indicate that the user has terminated, by changing the user's organization level to a suspense level. Additionally, the user ID is reset so that the user will no longer have access to utilize the account. On an annual basis GovTrip user accounts are reviewed by Customer Agency Travel Contacts. TSD System Administrators create reports of GovTrip users and distribute the reports to Customer Agency Travel for review and verification of the accounts.

Gov Trip has user access levels that separate permissions from highest to lowest into these categories:

- System administrators (NGMS only)
- Application administrators; Senior Systems Analysts
- Application administrators; Junior Systems Analysts
- Application administrators; Customer Service Help Desk Tier 2 and Junior Systems Analysts
- Approving Officials and Budget Reviewers
- Customer Service Help Desk Tier 1 and Accounting Technicians
- User; Traveler and Document Preparer
- Terminated Users; Invitational Travelers

Access privileges are granted in accordance with the concept of least privilege.

Users must establish their own unique GovTrip password. User passwords expire every 90 days, requiring the user to choose a new password. Failure to provide the appropriate password after three attempts will lock the user out of the system. The user must contact the TSD Travel Helpdesk where a System Administrator will contact NGMS to reset the GovTrip password, or the user can choose to wait one hour for GovTrip to automatically unlock the account. If the user's current session is inactive for 15 consecutive minutes, they will be timed out of the system and will have to log back into GovTrip. Passwords must be a combination of eight or more alpha/numeric characters; must include at least one uppercase, two lowercase, one number, and one special character. Passwords cannot be used again within four, ninety-day cycles.

Customer Agency Control Considerations

Customer Agencies should establish controls to:

- Review and approve listing of users with current ORACLE, Discoverer, PRISM, webTA, and GovTrip access to ensure appropriateness.

- Ensure exiting employee timecards are coded "Final" as this will help ensure that HR staff deactivate the employee's webTA access.

Tests of Operating Effectiveness and Results of Testing

- Inspected the Treasury Information Technology Security Program TDP-85-01 Volumes I and II and determined that security policies and procedures were documented.

- Inspected ORACLE user account management procedures and password procedures and determined that security policies and procedures were documented for ORACLE.

- Inquired of ARC management and observed a user log into ORACLE. Determined that connections to ORACLE were encrypted utilizing 128-bit SSL encryption.

- For a selection of new ORACLE users, inspected user access request forms and determined that the forms were completed and access was authorized.

- For a selection of changes to ORACLE user profiles, inspected authorizing documentation and determined that updates to access rights were authorized.

- Inspected a list of separated employees and for a selection of users, inspected a list of ORACLE application users, ORACLE server users, and ORACLE database users. Determined that separated employees did not retain access to the ORACLE application, server, or database, except as noted below:

  - The PRISM 120-day report of inactive users did not include users that had never logged into PRISM. ARC has since modified the 120-day inactivity report to capture PRISM users that have never logged in and have at least 120 days of inactivity since their user IDs were created or were last provisioned with access. ARC has a compensating control which aids in ensuring that any terminated PRISM users missed by the 120-day inactivity report review were removed. Specifically, ARC annually sends out lists of PRISM users to customer agencies for customers to verify that current users should have access. The customer agencies respond to ARC and identify any users whose access should be revoked.

- Inquired of ARC management and inspected evidence of distribution of ORACLE user lists for review and determined that user account lists were distributed on an annual basis for review.

- For a selection of customer agencies, inspected response to annual review of ORACLE user accounts and inspected a list of ORACLE users, and determined access was revoked for those user IDs marked for deletion.

- Inspected the list of operating units in ORACLE and determined that each Customer Agency was configured as a distinct operating unit. Additionally, for a selected user, inspected a list of operating units that the user had access to, observed the user access data within ORACLE, and noted that their access was restricted to the data records for operating units to which they were assigned access.

- Inspected a list of users with ORACLE System Administrator privileges and inquired of ARC management and determined that access privileges were commensurate with job responsibilities.

- Inspected the user roles assigned to the ORACLE System Administrators and compared them to a list of authorized functions required to perform end-of-month responsibilities and the BTD Allowable Responsibilities Table and determined that functional user permissions were restricted commensurate with job responsibilities.

- Inspected the access control lists for the ORACLE database and the host server and inquired of ARC management, and determined that the System Administrator and Database Administrator (DBA) privileges were commensurate with job responsibilities.

- Inspected ORACLE profile options and determined that ORACLE was configured to disconnect sessions if they remained inactive for 15 minutes (the setting is 30 consecutive minutes for the United States Mint's instance of ORACLE).

- Inspected ORACLE profile options, and determined that failed logins, password complexity, generation, and length requirements were configured in accordance with ARC password standards.

- For a selection of ORACLE system administrators and users, inspected the password lifespan days established for the individual users and determined that they were configured in accordance with ARC password standards.

- For a selection of dates, inspected ORACLE violation logs and evidence of review and determined that violations logs were reviewed.

- For a selection of dates, requested evidence of follow up e-mails sent to ORACLE users with excessive invalid access attempts and noted the following exception:

  - Of the 43 selected dates, 30 dates had excessive access attempts. E-mails were not disseminated to users with excessive access attempts on 2 of the dates selected.

- Inquired of management and observed an ORACLE System Administrator attempt to add responsibilities to their user ID, and determined that system administrators could not add responsibilities to their user IDs.

- Inspected evidence of review of ORACLE functional access privilege change logs, and determined that changes to functional access privileges assigned to ORACLE user accounts were reviewed daily by the PRISM Support team, except as noted below:

  - During testing of the reviews of access grants to ORACLE Federal Financials, it was determined that from a selection of 21 dates, evidence of review of ORACLE Federal Financials access grant logs could not be provided for 1 date selected.

- Inspected PRISM user account management procedures and password procedures and determined that security policies and procedures were documented for PRISM.

- Inquired of ARC management and observed a user log into PRISM and determined that connections to PRISM were encrypted utilizing 128-bit SSL encryption.

- For a selection of new PRISM users, inspected user access request forms and determined that the forms were completed and access was authorized.

- For a selection of changes to PRISM user accounts, inspected authorizing documentation and determined that updates to the accounts were authorized.

- Inspected a list of separated employees, and inspected a list of PRISM users, PRISM server users, and PRISM database users and determined that separated employees did not retain access to the PRISM application, server, or database.

- Inquired of ARC management and inspected evidence of distribution of PRISM user lists for review and determined that user account lists were distributed on an annual basis for review.

- For a selection of customer agencies, inspected response to annual review of PRISM user accounts and inspected a list of PRISM users, and determined access was revoked for those user IDs marked for deletion.

- Inspected the list of operating units in PRISM and determined that each Customer Agency was configured as a distinct operating unit. Additionally, for a selected user, inspected a list of operating units that the user had access to, observed the user access data within PRISM, and noted that their access was restricted to the data records for operating units to which they were assigned access.

- Inspected the access control lists for the PRISM backend database and the host server and inquired of ARC management, and determined that the System Administrator and DBA privileges were commensurate with job responsibilities.

- Inspected PRISM configuration settings and determined that PRISM sessions were configured to time-out if they remained inactive for 15 minutes.

- Inspected PRISM password settings and determined that failed logins, password complexity, aging, generation, and length requirements were configured in accordance with ARC password standards.

- For a selection of dates, inspected PRISM violation logs and evidence of review and determined that violations logs were reviewed, with exception to the issue noted below:

  - Of the 34 selected dates, evidence of review of PRISM violation logs could not be located for 1 of the dates selected.

- For a selection of dates, requested evidence of follow up e-mails sent to PRISM users with excessive invalid access attempts and determined that follow up e-mails were distributed, with exception to the issue noted below:

  - Of the 34 selected dates, 27 dates had excessive access attempts. E-mails were not distributed to users with excessive access attempts for 1 of the 27 selected dates with excessive access attempts.

- Inspected webTA user account management procedures and password procedures and determined that security policies and procedures were documented.

- Inquired of ARC management and observed a user log into webTA and determined that connections to webTA were encrypted utilizing 128-bit SSL encryption.

- For a selection of new webTA users with elevated privileges, inspected user access request forms and determined that the forms were completed and access was authorized

- For a selection of changes to webTA user profiles, inspected authorizing documentation and determined that updates to the accounts were authorized, except as noted below:

  - During testing of a selection of 60 access privileges, we determined that a single HR administrator granted 4 individuals access to additional instances of webTA not specified in their access forms..

- Inspected a list of separated employees and a list of webTA users, webTA server users, and webTA database users and determined that separated employees did not retain access to the webTA application, server, or database.

- Inquired of ARC management and inspected evidence of distribution of a list of webTA supervisors and timekeepers for review and determined that user account lists of supervisors and timekeepers were distributed on an annual basis for review.

- For a selection of customer agencies, inspected response to annual review of webTA user accounts and inspected a list of webTA users, and determined access was revoked for those user IDs marked for deletion.

- Inspected the access control lists for webTA and inquired of ARC management, and determined that privileges were commensurate with job responsibilities, except as noted below:

  - One individual from a list of 35 System and HR Administrators still had HR Administrator privileges after transferring to a different job within ARC that was not commensurate with their previous job responsibilities.

- Inspected the access control lists for the webTA backend database and the host server and inquired of ARC management, and determined that the System Administrator and DBA privileges were commensurate with job responsibilities.

- Inspected webTA password settings and determined that failed logins, password complexity, aging, generation, and length requirements were configured in accordance with ARC password standards.

- Inspected webTA configuration settings and determined that webTA sessions were configured to time-out if they remained inactive for 15 minutes.

- Inspected GovTrip user account management procedures and password procedures and determined that security policies and procedures were documented.

- For a selection of new GovTrip users, inspected user access request forms and determined that the forms were completed and access was authorized.

- For a selection of changes to GovTrip users, inspected authorizing documentation and determined that access changes were documented and access was authorized.

- Inspected a list of separated employees and a list of GovTrip users, and determined that separated employees did not retain access to the GovTrip application.

- Inquired of ARC management and inspected evidence of distribution of GovTrip user lists for review and determined that user account lists were distributed on an annual basis for review.

- For a selection of customer agencies, inspected response to annual review of GovTrip user accounts and inspected a list of GovTrip users, and determined access was revoked for those user IDs marked for deletion.

- Inquired of management and inspected a list of GovTrip users with elevated access privileges and compared them to an organization chart, and determined that privileges were commensurate with job responsibilities.

No exceptions noted, except as described above.

Control Objective 14 – System Changes

Controls provide reasonable assurance that system changes are tested, approved, and documented in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures for testing, approving, and documenting changes. ARC Support Desk staff serve as facilitators of the formal change management process, including administration of the ARC Change Management System (CMS) and documentation of the process itself. The ARC CMS is Commercial-Off-The-Shelf (COTS) software that was customized to meet ARC's needs.

<u>ORACLE and PRISM</u>
For ORACLE and PRISM, ARC uses CMS to document key steps for each change: including the initial request, approval, and implementation into production.

ARC processes standard software releases (i.e., patches) for both ORACLE and PRISM. Additionally, ARC processes customized application extension changes to ORACLE. The ability to process and apply ORACLE and PRISM changes is restricted to the database administrators under the coordination of OIT.

The system owner, or designee, has responsibility for initiating change requests. OIT has responsibility for maintaining all documentation with regard to system configurations and baselines. Change requests and approvals are documented in CMS.

ARC System Administrators, as designees of the system owner, serve as the primary initiators of change requests. The following is indicated in the request: all the affected parties, a description of the change, the applicable instance, and the requested date of the change. QCB staff develop and test the change in separate development and test instances. Changes are tested by running test scripts and analyzing the results. Upon successful completion of testing, QCB staff approve the change request and forward it to the performer of the change, generally OIT database administrators. After the approved request has been completed, the performer updates the request in CMS accordingly, and the request is then closed.

For emergency changes to a production instance of ORACLE or PRISM, ARC requires verbal approval from a designated on-call manager and from the Information Technology Support Branch Manager. ARC Support Desk staff document the emergency change in CMS on the next business day. No emergency changes were implemented during the 2007 examination period.

<u>webTA</u>
ARC has a webTA maintenance agreement in place with immixTechnology, a vendor for Kronos' webTA product.

For webTA, ARC applies standard software releases (i.e., patches) only. Unlike ORACLE, webTA does not have application extensions that are customizable by ARC.

When a new webTA release is received from Kronos (the developer of webTA), QCB staff test the new release in a separate test instance by running test scripts and analyzing the results. Upon successful completion of customer acceptance testing, the QCB staff forward a request for applying the new webTA release to production to the appropriate parties for approval. The ability to apply webTA releases is restricted to the database administrators under the coordination of OIT. The new webTA release is not applied to production until it has been successfully tested and approved.

Gov Trip

GovTrip is hosted and maintained by NGMS at their facility. NGMS informs the TSD of scheduled updated system releases and the changes contained therein. System changes are also initiated by TSD Analysts who make enhancement requests to NGMS for changes to be included by NGMS in future scheduled release updates. TSD analysts test all GovTrip changes in a GovTrip acceptance test environment. If any of the changes included in a scheduled GovTrip release update fail TSD's acceptance testing, NGMS may delay implementation of the release update. TSD has documented procedures for testing GovTrip changes. Guidance is provided to customer contacts on any changes.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for change controls and determined that the change control procedures including documenting, testing, and approving changes were documented.

- Inspected a list of users with access to the ORACLE and PRISM applications and database servers and inquired of ARC management and determined that access to make changes was commensurate with job responsibilities.

- For a selection of ORACLE and PRISM changes, inspected supporting authorization documentation and determined that change approvals were recorded within CMS.

- For a selection of ORACLE and PRISM changes, inspected documentation of testing and determined that the changes were tested prior to implementation in production.

- Inspected the webTA system maintenance agreement and determined that it contained system maintenance provisions and that it was current.

- For a selection of webTA upgrades, inspected testing and authorization documentation and determined that documentation of testing and approval was documented.

- For a selection of GovTrip changes, inspected documentation of testing and determined that changes were tested prior to implementation in production.

No exceptions noted.

Control Objective 15 – Suppliers and Banks Record Changes

Controls provide reasonable assurance that changes made to Suppliers and Banks records require appropriate system access and the changes are reviewed, approved, and documented in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures related to Suppliers and Banks record changes for staff to follow.

Segregation of Duties – Changes to Suppliers and Banks Records
User profiles set by ORACLE system administrators, as authorized by the user's supervisor or manager, ensure that only authorized Central Accounting Branch (CAB) employees are able to make changes to Suppliers and Banks records. Authorized CAB employees who have Suppliers and Banks record change privileges do not have authorization to approve vendor payments in the accounting systems allowing for proper segregation of duties.

Changes to Suppliers and Banks records that include taxpayer identification number, address, or bank routing/account number require:

- A source document (Central Contractor Registration (CCR) database or a document supplied by the vendor or customer, when CCR is not applicable. – i.e., grants and loans, payroll database, and/or e-mail, etc.),
- Initials of the employee processing the change, and
- Independent review.

Review – Changes to Suppliers and Banks Records
CAB employees review and process changes to Suppliers and Banks records and maintain the supporting source documentation as described above.

A reviewing CAB employee compares changes to Suppliers and Banks records from the ORACLE system to the change request documents and initials the audit report indicating review. The reviewing employee does not have access to make changes to Suppliers and Banks records in ORACLE. Therefore, if errors were made, the reviewing CAB employee would provide a copy of the source document to an authorized employee for correction and subsequent review.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for Suppliers and Banks record changes and observed ARC staff change Suppliers and Banks records and determined that the processing was in accordance with the procedures.

- Inspected a list of ORACLE users who have been assigned the ORACLE responsibilities with the ability to make changes to Suppliers and Banks records and determined that all users with such access were authorized CAB employees.

- Inspected a list of ORACLE users who have privileges to approve vendor payments and compared it to the list of users who have privileges to make changes to Suppliers and Banks records and determined that none of the users were granted system privileges to both change Suppliers and Banks records and approve vendor payments.

- For a selection of changes to Suppliers and Banks records, inspected the reviewed audit report and sign-off by the reviewing employee and determined that the Suppliers and Banks record changes were reviewed and approved.

- For each reviewing employee, inspected the list of users with ORACLE responsibilities that grant access to change Suppliers and Banks records and determined that reviewing employees did not have privileges to change Suppliers and Banks records.

No exceptions noted.

Control Objective 16 – Non-interruptive System Service

Controls provide reasonable assurance that interruption due to operational failures are appropriately limited.

Description of Controls

The ORACLE, PRISM, and webTA servers reside in OIT's data center at the BPD's main building located at 200 Third Street in Parkersburg, West Virginia. Armed security guards man and monitor the north entrance to the building 24 hours a day, 7 days a week. Armed security guards also man and monitor the south entrance when it's open, which is from 5:30 am to 6:00 pm on work-days. In addition, an armed roving patrol security guard makes interior and exterior foot patrols 24 hours a day, 7 days a week. A digital video camera system monitors all entrances, the building perimeter, and certain interior areas, including the data center, and records activity 24 hours a day. Physical access to the OIT Data Center is restricted to authorized employees only. ARC employee access requires ARC branch management and ARC support desk approval. The request is forwarded to OIT's data center managers for approval in the workflow application, iET Enterprise. If OIT approves the request in iET Enterprise, the BPD Division of Security and Emergency Preparedness (DSEP) Security Branch grants access to the data center on the individual's ID badge, using the Momentum Access Control System. Each badge swipe on the card reader provides an audit trail of employees who have accessed the facility, which is reviewed by OIT management for potential access violations. Individuals without badge access to the data center are required to sign in/out of a logbook, and provide a valid reason for accessing the data center. Once the entry log is reviewed, access to the data center is either granted or denied.

Beginning in June 2007, OIT performed a semiannual reconciliation of individuals with data center access (as recorded in Momentum) to individuals authorized to have data center access (as recorded in iET Enterprise). If an individual is found to have unauthorized data center access, OIT will, based on the individual's need for access, make a decision whether to request that DSEP remove their data center access in Momentum or whether to provide authorization for their access. Additionally, OIT performs a rolling annual review and recertification of individuals with access to the data center. The review is performed by branch, according to a monthly schedule. During the course of a year, each person who has had authorized data center access for at least one-year, will have their access reviewed and recertified. For any individuals that OIT determines have unnecessary data center access, OIT instructs DSEP to remove their data center access from their ID badge.

The ORACLE application is monitored using Quest's Spotlight and Foglight. Performance monitoring is provided by Fluke Networks SuperAgent. The networked applications also use Mercury's Site Scope to monitor web sites, FTP servers, web servers, and some intrusion detection every ten minutes. The availability of network infrastructure, such as switches and firewalls, is monitored using HP Openview. OIT's data center is also physically monitored by Andover monitoring software. The Andover monitoring software provides continuous checking and alarming capabilities for temperature changes, water, and humidity threats. Fire detection and suppression systems are installed in the data center. Redundant battery-powered uninterruptible power supplies and a backup generator protect the data center from an unplanned loss of power. Redundant air conditioning systems protect data center computers from overheating in the event of air conditioning equipment failure. OIT provides operations, support, capacity planning, performance monitoring, networking, security monitoring, development, change management, back up, hardware acquisitions and maintenance, and installation support for ARC.

ORACLE

System operations manuals are provided to each employee assigned system maintenance responsibilities. In addition, ORACLE support personnel have access to internal application setup and security documentation, as well as various manuals and documentation produced by ORACLE Corporation. The ORACLE Support Team is available for users to call if they are experiencing difficulties with the system. The ORACLE Support Team acts as a liaison between the user and OIT to resolve system issues.

At no less frequently than 15-minute intervals, the ORACLE production system is automatically replicated to the off-site ORACLE CONTINGENCY server. The ORACLE CONTINGENCY server is tested annually as part of an ORACLE continuity of operations (COOP) exercise.

Production system backups are performed nightly to disk. OIT performs complete backups of the AppTier and database nightly. These backups are copied into two separate locations (CONTINGENCY and SUPPORT servers) for failover and redundancy. SUPPORT is used by CSB and QCB to troubleshoot LIVE issues. Additionally, OIT performs differential backups of the production system nightly and performs a full tape backup weekly. The daily backup tapes are sent to an offsite facility on a weekly basis where they are kept for eight weeks. The monthly backup tapes are then sent to a long-term offsite facility. See Control Objective 17 for further discussion of the backup process.

PRISM

PRISM support personnel have access to internal application setup and security documentation, as well as various manuals and documentation produced by Compusearch Corporation. The PRISM Support Team within CSB is available for users to call if they are experiencing difficulties with the system. The PRISM Support Team acts as a liaison between the user and OIT to resolve system issues.

At not no less frequently than 15-minute intervals, the PRISM production system is automatically replicated to the off-site PRISM CONTINGENCY server. The PRISM CONTINGENCY server is tested annually as part of an ORACLE continuity of operations (COOP) exercise.

OIT performs differential backups of the production system nightly and performs a full tape backup weekly. The nightly backup tapes are sent to an offsite facility on a weekly basis where they are kept for eight weeks. The monthly backup tapes are then sent to a long-term offsite facility. See Control Objective 17 for further discussion of the backup process.

webTA

webTA support personnel have access to online documentation produced by Kronos. The Human Resources Support Desk is available for users to call if they are experiencing difficulties with the system. QCB acts as a liaison between the Human Resources Support Desk and OIT to resolve system issues.

OIT performs differential backups of the production system nightly and performs a full tape backup weekly. The nightly backup tapes are sent to an offsite facility on a weekly basis where they are kept for eight weeks. The monthly backup tapes are then sent to a long-term offsite facility. See Control Objective 17 for further discussion of the backup process.

Gov Trip
ARC TSD analysts investigate any system issues noticed by the ARC staff or reported to TSD by GovTrip users. When possible, TSD analysts resolve GovTrip issues. If the TSD Analyst cannot resolve an issue, the issue is escalated to a TSD Administrator. If the TSD Administrator cannot resolve an issue, the issue is escalated to NGMS. TSD notifies system users of the length of the expected outage or malfunction and notifies them again when the issue is resolved.

NGMS maintains the data in their Business Data Warehouse for six years and three months.

Tests of Operating Effectiveness and Results of Testing

- Observed the north and south entrances of the 200 Third Street building during normal business hours and noted that guards were on duty.

- Observed the digital video camera surveillance system and noted that the system was operating as designed and activity was continuously recorded.

- Observed entrances to the OIT data center and noted that all entrance doors were controlled by card readers and were locked.

- For a selection of employees granted access to the OIT datacenter, inspected physical access approvals and inquired of ARC management and determined that data center access was authorized and was commensurate with job responsibilities.

- For a selection of branches, inspected documentation of the annual review of physical access privileges to the datacenter and determined that access privileges were reviewed, except as noted below.

  - The review of datacenter access privileges was performed using the workflow system that is utilized to approve datacenter access, and not a list of individuals generated from the physical access control system. Inquired of OIT management and was informed that an undocumented reconciliation was performed, however the process did not constitute a formally-documented reconciliation of the workflow approval system to the physical access control system.

  - Inspected a list of all individuals with data center access (queried from Momentum) and reconciled it to a list of individuals authorized to have data center access (queried from iET Enterprise) and determined 13 individuals had unauthorized access to the BPD data center. Inquired of BPD management and were informed that for 9 of the 13 individual's access to the data center was appropriate, but not properly documented. We were further informed that the remaining 4 individuals had no need for access to the datacenter.

- Inspected documentation of OIT's semiannual reconciliation of individuals with data center access to individuals authorized to have data center access performed in June 2007 and determined that OIT performed reconciliation in June 2007.

- Inspected a list of all individuals with data center access, as of June 30, 2007 (queried from Momentum) and reconciled it to a list of individuals authorized to have data center access (queried from iET Enterprise) and determined that no individuals had unauthorized access to the BPD data center.

- For a selection of months, inspected OIT card-key audit reports and the e-mail distribution of the reports and determined that access attempts were logged and that the reports were reviewed by OIT management for potential access violations.

- Observed visitor access to the data center and noted that visitors were required to sign a logbook, provide a reason for access, and were escorted while in the data center.

- For a selection of months, inspected a selection of noncard-key data center visitation logs and determined that the logs were in use.

- Inquired of OIT staff and observed Quest's Spotlight and Foglight, Fluke Networks SuperAgent, and Mercury's Site Scope, and noted that these applications were installed and in use by OIT staff.

- Inquired of OIT staff and observed variance reports, monitoring logs, and automatically generated alerts from Quest's Spotlight and Foglight and noted that these applications provided monitoring over ORACLE and that OIT staff reviewed these reports, logs and alerts.

- Inquired of OIT staff and observed variance reports, monitoring logs, and automatically generated alerts from Fluke Networks SuperAgent and noted that these applications provided monitoring over the general performance of networked applications and that OIT staff reviewed these reports, logs and alerts.

- Inquired of OIT staff and observed variance monitoring logs and automatically generated alerts from Mercury's Site Scope and noted that this application provided monitoring over websites, FTP servers, and web servers and that OIT staff reviewed these logs and alerts.

- Inquired of OIT staff and observed the Andover monitoring application and noted that the application was installed and used to monitor OIT data center environmental conditions.

- Observed the OIT data center and noted that sprinklers, hand-held fire extinguishers, and raised floors were present.

- Inspected completed maintenance work orders and inspection reports for the fire alarm system, the fire suppression system, the uninterruptible power supply (UPS), and the emergency power generator and determined that the fire alarm system, fire suppression system and the generator and UPS were maintained.

- Inquired of management and inspected system operations manuals for ORACLE and determined that the manuals were available to support personnel.

- Inquired of management and was informed that the ORACLE Support Team fielded calls for incidents related to ORACLE.

- Inquired of management and inspected PRISM application setup and security documentation and system manuals and determined that documentation was available to support personnel.

- Inquired of management and was informed that the PRISM Support Team fielded calls for incidents related to PRISM.

- Inspected ARC’s maintenance agreement for webTA and determined that it was current.

- Inquired of management and was informed that the ARC Support Desk fielded calls for incidents related to webTA.

- Inspected the GovTrip incident escalation procedures and inquired of TSD management and determined that the incident escalation procedures were documented and available to support personnel.

No exceptions noted, except as described above.

Control Objective 17 – Records Maintenance

Controls provide reasonable assurance that source document files are properly retained and safeguarded in accordance with ARC and BPD's Records Management Office policies and procedures.

Description of Controls

OIT completes backups during scheduled maintenance periods, which are after normal work hours. When the backups are complete, OIT retains the tapes at the data center for no more than one week before the tapes are sent to local offsite storage at a BPD contingency site. After an additional week, OIT sends the weekly full backup tape to long-term offsite storage, where they are retained six and one-half years according to the General Records Schedule issued by the National Archives and Records Administration. Tapes sent offsite are recorded on a tracking sheet in the Tape Management System. After four weeks at local offsite storage, the daily differential tapes are then returned to the data center where they are recycled. Long-term offsite storage is provided through a contract with Iron Mountain. Authority to recall tapes from off-site is limited to those individuals whose job responsibilities require access to backup tapes.

When tapes are returned from long-term storage by Iron Mountain, OIT reconciles the shipment that they have received to their records of the tapes expected to be returned.

On an annual basis, OIT performs a full physical inventory of all backup tapes that are in BPD's possession, both at the 200 Third Street data center tape library in Parkersburg, West Virginia and at the BPD's contingency site.

Network File Servers

Differential tape backups of network servers are created daily. On a weekly basis, OIT completes a full back up of all ARC shared network files (active and inactive) to a data tape. OIT retains the backups tapes for five weeks.

ORACLE

At no less frequently than 15-minute intervals, the ORACLE production system is automatically replicated to the off-site ORACLE CONTINGENCY server. The ORACLE CONTINGENCY server is tested annually as part of an ORACLE continuity of operations (COOP) exercise.

Production system backups are performed nightly to disk. OIT performs complete backups of the AppTier and database nightly. These backups are copied into two separate locations (CONTINGENCY and SUPPORT servers) for failover and redundancy. SUPPORT is used by CSB and QCB to troubleshoot LIVE issues. Additionally, OIT performs differential backups of the production system nightly and performs a full tape backup weekly. The daily backup tapes are sent to an offsite facility on a weekly basis where they are kept for eight weeks. The monthly backup tapes are then sent to a long-term offsite facility.

PRISM

OIT performs differential backups of the production system nightly and performs a full tape backup weekly. The nightly backup tapes are sent to an offsite facility on a weekly basis where they are kept for eight weeks. The monthly backup tapes are then sent to a long-term offsite facility. The PRISM CONTINGENCY server is tested annually as part of an ORACLE continuity of operations (COOP) exercise.

webTA

OIT performs differential backups of the production system nightly and performs a full tape backup weekly. The nightly backup tapes are sent to an offsite facility on a weekly basis where they are kept for eight weeks. The monthly backup tapes are then sent to a long-term offsite facility.

Gov Trip

NGMS maintains the data in their Business Data Warehouse for six years and three months.

Hard copy data records

Hard copy data records are kept in folders and/or binders on-site for one or two years. When hard copy data records are ready to be transferred off-site, they are packed into boxes to be sent to off-site storage. Prior to sending the boxes off-site, a description of the data being stored in the box, including the box's latest document date, and approved retention authority is entered into the Records Management System called FileSurf. The Records Management Office approves the box for storage and produces a label that is placed on the box. The label includes a unique box number, bar code and box description and the destruction date. The destruction date is calculated by the system using the approved retention period from the latest document date. Once the boxes are sent off-site by OMS's Information Management Branch (IMB), the records can be requested using FileSurf, which is maintained by IMB.

Tests of Operating Effectiveness and Results of Testing

- Inspected backups procedures and determined that backup procedures including schedules and retention periods were documented.
- Inspected the agreement with the offsite storage vendor and determined that a formal agreement was in place for the offsite storage of media.
- Inspected backup rotation logs and determined that backups were rotated offsite.
- Inspected a list of individuals with authority to recall tapes from offsite storage and inquired of ARC management and determined that authority to recall tapes was commensurate with job responsibilities.
- For a selected network file server used by ARC, inspected system-generated backup schedules and backup logs and determined that daily differential backups and weekly full backups of the file server were scheduled and completed.
- Inspected system-generated backup schedules and backup logs for ORACLE and determined that daily differential backups and weekly full backups were scheduled and completed.

- Inquired of OIT staff and inspected documented test results from the annual ORACLE COOP exercise and determined that the ORACLE CONTINGENCY server had been successfully tested in March 2007.

- Inspected system-generated backup schedules and backup logs for PRISM and determined that daily differential backups and weekly full backups were scheduled and completed.

- Inquired of OIT staff and inspected documented test results from the annual PRISM COOP exercise and determined that the PRISM CONTINGENCY server had been tested in March 2007.

- Inspected system-generated backup schedules and backup logs for webTA and determined that daily differential backups and weekly full backups were scheduled and completed.

- Observed the location of the hard copy records and noted that hard copy records were stored in a secure warehouse.

- Inspected hard copy records offsite shipment logs and determined that the hard copy records were shipped offsite.

- For a selection of boxes from the hard copy records offsite shipment logs, inspected the selected box at the warehouse and determined that hard copy records recorded as shipped offsite were stored at ARC's secure warehouse.

No exceptions noted.

IV. OTHER INFORMATION PROVIDED BY THE BUREAU OF THE PUBLIC DEBT

CONTINGENCY PLANNING

System Back Up

The ORACLE Federal Financials (ORACLE) accounting system has a contingency plan managed by the Administrative Resource Center (ARC). There is a formal ARC disaster recovery plan (DRP), last updated August 2005. All essential ORACLE functions will be performed at the contingency site with the support of ARC employees. Monthly testing is conducted that focuses on the restoration of systems, as well as critical data sets. Full disaster recovery testing is performed on an annual basis in conjunction with the Bureau of the Public Debt's (BPD) Office of Information Technology (OIT) Data Center's DRP.

OIT uses the NetBackup from Veritas to backup networked systems. Short-term storage of the core accounting system tapes are maintained at the Contingency Automated Processing Site (CAPS) facility in Mineral Wells, West Virginia. Long-term tape storage is maintained at an offsite location in Pennsylvania.

OIT performs changed data backups of the ORACLE and PRISM systems daily and performs full data backups weekly. Daily differential backup tapes are retained by OIT and stored in the Data Center where they are recycled after four weeks. On a weekly basis, the full tape backups are placed in turtle cases and sent to the Tape Vault at the CAPS facility. The tape backups are retained for approximately eight weeks and then shipped to the long-term storage facility in Pennsylvania where they are retained for seven years.

OIT performs full backups of ORACLE LIVE and AppTier nightly. These backups are copied into two separate locations (CONTINGENCY and SUPPORT servers) for contingency purposes. SUPPORT is used by CSB and QCB to troubleshoot LIVE issues. CONTINGENCY is tested daily by the database administrators in OIT. All critical datasets are retained for at least six years and three months.

At 15-minute intervals, the ORACLE production system is automatically replicated to the off-site ORACLE CONTINGENCY server. The ORACLE CONTINGENCY server is tested semi-annually as part of an ORACLE contingency exercise.

OIT performs differential backups of the webTA production system nightly and performs a full tape back up weekly. The nightly backup tapes are sent to an offsite facility on a weekly basis where they are kept for eight weeks. The monthly backup tapes are then sent to a long-term offsite facility.

NGMS is responsible for system backup of GovTrip and maintains data in their Business Data Warehouse for six years and three months.

Continuity of Operations

A fire alarm and sprinkler system that is managed, maintained, and tested by the facilities management department at BPD protects the Avery Street and Third Street facilities. Alarms are active 24 hours a day, 7 days a week, and are tied-in to the local fire department over phone lines for spontaneous notification. Sprinkler heads are located in the ceiling of each room of the buildings. This is a "wet pipe" (always charged with water) system with individual heads that discharge water.

In the event the main building, where the ORACLE system is maintained, becomes inoperable, network operations would be relocated to the CAPS facility in accordance with the OIT data center’s DRP. This facility employs a “warm site” strategy for recovery of network operations. The ORACLE accounting system has been classified as a critical application.

As part of the ARC DRP, should the Avery Street become unavailable, ARC personnel will relocate to the CAPS facility to reestablish their essential operations. BPD will revert to manual procedures until the networked accounting system is fully recovered at the CAPS facility.

V. INDEPENDENT AUDITORS’ REPORT ON COMPLIANCE WITH LAWS AND REGULATIONS

KPMG

KPMG LLP
2001 M Street, NW
Washington, DC 20036

Independent Auditors' Report

Inspector General, U.S. Department of the Treasury
Deputy Executive Director, Administrative Resource Center:

We have examined the accompanying description of the accounting processing and general computer controls related to the financial management services provided by the Administrative Resource Center (ARC) of the Bureau of the Public Debt (BPD) as of June 30, 2007, and have issued our report thereon dated July 20, 2007. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants, and applicable *Government Auditing Standards*, issued by the Comptroller General of the United States.

Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of BPD's controls that may be relevant to a Customer Agencies' internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and Customer Agencies and sub-service organizations applied the controls contemplated in the design of BPD's controls; and (3) such controls had been placed in operation as of June 30, 2007. The control objectives were specified by BPD. Our examination included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

Compliance with laws and regulations applicable to ARC of BPD is the responsibility of BPD management. As part of obtaining reasonable assurance about whether control structure policies and procedures tested were operating with sufficient effectiveness to achieve the related control objectives during the period from July 1, 2006 to June 30, 2007, we performed tests of BPD's compliance with certain provisions of applicable laws and regulations directly and materially affecting the accounting and general computer controls. We limited our tests of compliance to these provisions and we did not test compliance with all applicable laws and regulations. The objective of our examination was not, however, to provide an opinion on overall compliance with such provisions. Accordingly, we do not express such an opinion.

The results of our tests disclosed no instances of noncompliance that are required to be reported herein under *Government Auditing Standards*.

This report is intended solely for the information and use of the management of BPD, its Customer Agencies, the independent auditors of its Customer Agencies, U.S. Department of the Treasury Office of Inspector General, Office of Management and Budget, Government Accountability Office, and the U.S. Congress, and is not intended to be, and should not be, used by anyone other than these specified parties.

KPMG LLP

July 20, 2007